uc3m | Universidad Carlos III de Madrid

Grado Universitario en Ingeniería Telemática

2018-2019

Trabajo Fin de Grado

"Diseño de una práctica para la enseñanza de redes privadas virtuales de capa 3 (L3VPN) con MPLS"

Andrea Ruiz Pedraza

Tutor

David Larrabeiti López

Julio 2019

RESUMEN

La presente Memoria corresponde al estudio de las tecnologías VPN sobre MPLS. El estudio comienza con una introducción a estas tecnologías para después desarrollar una práctica VPN de capa 3, la cual pueda ser usada posteriormente en docencia de grado o máster.

Primeramente, se pretenden estudiar las características que definen una red MPLS VPN, tanto de nivel 3 como de nivel 2. Se comenzará por el protocolo MPLS, el cual conforma la red troncal, hasta las posteriores tecnologías VPN, las cuales establecen la comunicación con los clientes.

Una vez que todos los conceptos necesarios han sido estudiados, el trabajo se centra en el desarrollo de un ejemplo práctico de arquitectura MPLS VPN de nivel 3. En primer lugar, realizaremos el análisis y diseño de la topología a implementar y, en segundo lugar, veremos la propia implementación, en un emulador, de la nueva topología.

Por último, se crea un modelo de prácticas que pueda ser usado posteriormente como parte del plan de estudios de una asignatura de grado o máster. Para ello, como enunciado de la práctica, se exponen una serie de cuestiones relacionadas con la topología implementada. Además, para añadir un poco de complejidad a la práctica, se define una segunda topología, cuya implementación deberá completar el alumno. El objetivo de esta práctica es la enseñanza, de una manera más dinámica, de los conceptos que caracterizan una red MPLS VPN.

Se ha escogido la tecnología MPLS VPN como tema principal del ensayo debido a su gran popularidad entre las empresas tecnológicas, su creciente evolución dentro del sector y la cantidad de alternativas que ofrece. Asimismo, durante el desarrollo de proyecto, se han podido observar otras ventajas de esta tecnología como su gran escalabilidad, flexibilidad, rendimiento, optimización del ancho de banda y facilidad en su configuración -el uso del protocolo BGP hace que tengas que configurar muy pocos elementos de la red para añadir una nueva sede.

Palabras clave: Content distribution networks, multiprotocol label switching, virtual private networks, student activities, software testing.

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

LISTA DE ABREVIATURAS

BGP	*Border Gateway Protocol*
CE	*Customer Edge*
FIB	*Forwarding Information Base*
IGP	*Interior Gateway Protocol*
IP	*Internet Protocol*
LAN	*Local Area Network*
LDP	*Label Distribution Protocol*
LSP	*Label-switched Path*
MAC	*Media Access Control*
MAN	*Metropolitan Area Network*
MPLS	*Multiprotocol Label Switching*
OSPF	*Open Shortest Path First*
P2P	*Peer-to-peer*
P	*Provider*
PE	*Provider Edge*
QoS	*Quality of Service*
RIP	*Routing Information Protocol*
RD	*Route Distinguisher*
RT	*Route Target*
SP	*Service Provider*
TIC	Tecnologías de la información y la comunicación
VPLS	*Virtual Private LAN Service*
VPN	*Virtual Private Network*
VRF	*Virtual Routing and Forwarding*
WAN	*Wide Area Network*

1. Introducción

1.1 Motivación del trabajo

La tecnología MPLS VPN ha ganado hoy en día una inmensa popularidad entre las empresas del sector tecnológico. Esta aporta una solución a la interconexión entre los distintos equipos de una red.

Debido a la alta velocidad y el bajo coste que ofrecen respecto a otras redes VPN (*Virtual Private Network*), las plataformas MPLS VPN son usadas en muchos dominios.

Las redes MPLS VPN aseguran la comunicación entre distintos usuarios aislados geográficamente gracias a redes MAN (*Metropolitan Area Network*) y WAN (*Wide Area Network*), como si formaran parte de la misma LAN (*Local Area Network*).

Hoy en día, ya que estas redes ofrecen comunicaciones eficaces y seguras, sus aplicaciones van desde redes industriales hasta móviles. Asimismo, ofrecen la posibilidad, por ejemplo, de accesos remotos o de enlaces entre varias oficinas con nexo Internet.

En una topología MPLS VPN, gracias al conjunto de diversas tecnologías y a los correspondientes protocolos de control, se consigue privacidad en las redes de cada uno de los clientes.

No obstante, estas nuevas aplicaciones precisan de requisitos adicionales como seguridad, escalabilidad y fiabilidad mejoradas, simplicidad de uso y optimización de recursos.

Las necesidades del cliente final son las que dictan el diseño óptimo y eficiente a desarrollar siendo así el tipo de enlace y de conectividad elementos importantes de este análisis.

1.2 *Objetivos del trabajo*

El objetivo de este proyecto es realizar una introducción a las tecnologías VPN sobre MPLS para después desarrollar una práctica VPN de capa 3, la cual pueda ser usada posteriormente en docencia de grado o máster.

Primeramente, se pretenden estudiar las características que definen una red MPLS VPN, tanto de nivel 3 como de nivel 2. Se comenzará por el protocolo MPLS, el cual conforma la red troncal, hasta las posteriores tecnologías VPN, las cuales establecen la comunicación con los clientes.

Una vez que todos los conceptos necesarios han sido estudiados, el trabajo se centra en el desarrollo de un ejemplo práctico de arquitectura MPLS VPN de nivel 3. En primer lugar, realizaremos el análisis y diseño de la topología a implementar y, en segundo lugar, veremos la propia implementación, en un emulador, de la nueva topología.

Por último, se crea un modelo de prácticas que pueda ser usado posteriormente como parte del plan de estudios de una asignatura de grado o máster. Para ello, como enunciado de la práctica, se exponen una serie de cuestiones relacionadas con la topología implementada. Además, para añadir un poco de complejidad a la práctica, se define una segunda topología, cuya implementación deberá completar el alumno. El objetivo de esta práctica es la enseñanza, de una manera más dinámica, de los conceptos que caracterizan una red MPLS VPN.

1.3 *Marco regulador*

El sector de las telecomunicaciones es regulado de manera habitual. En la actualidad, este tipo de proyectos están regulados en España según el nuevo marco regulador de las telecomunicaciones. Este nuevo marco está formado por la Directiva 2002/21/CE, la 2002/77/CE y otras cuatro adicionales.

El servicio de VPN es un servicio de Telecomunicación sometido a esta normativa.

La Ley General de Telecomunicaciones es necesaria para garantizar la eficiencia del mercado y la protección de los derechos de los clientes. Esta regulación constituye un gran esfuerzo por conseguir principios generales que protejan al sector de la creciente y continua evolución del mercado.

1.4 *Entorno socioeconómico*

El sector de las Telecomunicaciones, desde hace unos años, ha experimentado una tendencia positiva de crecimiento social y económico. Elementos como el número de empresas dedicadas al sector, la inversión, los empleos activos o el volumen de negocio están en continuo auge.

En 2017, a nivel mundial, este sector obtuvo unos ingresos de más de 1.245.457 millones de euros, 1,4% más que en 2016. [17]

En España, sin embargo, todos estos elementos experimentan un declive respecto a años anteriores. Esta rama, dentro del sector TIC, es la única que percibe tendencia negativa. Aun así, gracias al gran incremento conseguido desde 2012, las cifras obtenidas la sitúan entre los puestos más altos de las secciones TIC: 3.632 fueron las empresas Telco en 2017, con unos ingresos totales de 27.904 millones de euros. [17]

La inversión realizada por parte de estas empresas en el sector es la cifra que más se ha visto afectada. Un 5,4% de descenso interanual supuso, en 2017, una pérdida de financiación de unos 265 millones de euros [17]. Por último, en el caso del volumen de negocio, aun habiendo disminuido, continúa siendo la cifra más alta del sector, siendo los servicios minoristas los mayores proveedores (78,6% del total).

Observando la continua tendencia positiva mundial, no se duda acerca de la prolongada evolución de todos los aspectos económicos y sociales del sector de las telecomunicaciones. Se estima que, en el periodo contenido entre 2017 y 2022, el crecimiento de todos los elementos citados sea constante, alcanzando así una tasa media de crecimiento del 1,5% por año.

En el caso de España, aun con los datos obtenidos en 2017, las previsiones son optimistas. Se vaticina una tendencia positiva, incluso mayor a la europea. Mientras que nuestro país se situaría cercano a la tasa media mundial, Europa solo alcanzaría

el 0,6% [17]. Este crecimiento puede estar relacionado con el auge en el interés hacia el comercio exterior de servicios y bienes TIC de nuestro país, así como, la creciente inversión proveniente de empresas TIC extranjeras.

1.4.1 Pronósticos y tendencias de tráfico IP

No se dispone de datos de tráfico VPN publicados por los diferentes operadores de telecomunicación. No obstante, se puede estimar que su evolución va emparejada al crecimiento del tráfico IP empresarial.

Según el "*Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper*", las previsiones para 2022 son extraordinarias ya que se estima un crecimiento mayor, en estos cinco años, que en toda la historia de Internet.

		2017	2022	TCAC (2017-2022)
Tráfico IP	Global	122 EB/mes	396 EB/mes	26%
	España	1,4 EB/mes	4,4 EB/mes	25%

Tabla 1. Tráfico IP 2017-2022 [18]

Como se puede observar en la Tabla 1, el tráfico IP superará en el año 2022 el triple del conseguido en 2017, resultando en su mayor parte tráfico de redes inalámbricas (71% del tráfico IP total en 2022). [18]

El tráfico IP se puede dividir en dos grandes grupos según el usuario final: **consumidores**, donde se incluye aquel tráfico IP generado por viviendas, universidades, etc.; y **negocios**, tráfico IP WAN o Internet generado por empresas y gobiernos. En 2022 se tasa en un 84% del tráfico IP total el primer grupo y en un 16% el segundo, siendo el tráfico Internet el destacado de ambos.

			2017	2022
Tráfico Internet	Consumidores *(57% del tráfico IP total en 2022)*	*Global*	77 EB/mes	293 EB/mes
		EU Occidental	12 EB/mes	37 EB/mes
	Negocios *(12% del tráfico IP total en 2022)*	*Global*	17,25 EB/mes	48,74 EB/mes
		EU Occidental	3,62 EB/mes	9,06 EB/mes

Tabla 2. Tráfico Internet 2017-2022 [18]

1.5 *Planificación*

En esta sección, se muestra la planificación total de la elaboración del proyecto.

A continuación, se puede observar el desglose, por partes, de esta planificación, así como sus correspondientes fechas de inicio y finalización y el número de jornadas dedicadas a cada etapa.

Tarea	Inicio	Finalización	Duración
Estudio	26 nov ‘18	2 abril ‘19	127 días
Plan	22 nov ‘18	25 nov ‘18	3 días
Implementación	10 ene ‘19	25 marzo ‘19	74 días
Pruebas	10 ene ‘19	28 marzo ‘19	77 días
Documentación	2 dic ‘18	3 mayo ‘19	152 días
TOTAL	**22 nov ‘18**	**3 mayo ‘19**	**163 días (~ 5,5 meses)**

Tabla 3. Planificación

2. Marco Teórico

2.1 MPLS (Multiprotocol Label Switching)

MPLS (*Multiprotocol Label Switching*) es un mecanismo de conmutación de WAN o red de área amplia basado en etiquetas. Permite controlar flujos de tráfico de principio a fin a mayor velocidad sin tener en cuenta únicamente la dirección destino.

La tecnología MPLS, asimismo, permite enviar los paquetes en el nivel 2 OSI, de enlace, apoyándose en la calidad del servicio que aporta la capa 3, de red, y por ello se le reconoce como un protocolo de nivel 2.5.

El camino que deben seguir los paquetes lo determina una cabecera especial llamada etiqueta, que se asigna a la entrada de la red y sirve como base al reenvío del tráfico.

Una etiqueta es básicamente un valor corto de tamaño fijo que funciona como identificador de conexión e informa a un router del trayecto al que pertenece el paquete. De esta manera, el router puede usar su interfaz de entrada y la información del trayecto para determinar cuál es el siguiente nodo. Esto hace que el tiempo de conmutación se reduzca.

MPLS permite a grupos de usuarios y aplicaciones ser agrupados dentro de una etiqueta y, si es requerido, proveer sus propios servicios de manera separada. Además, al encapsular los datos en la etiqueta, estos usuarios o aplicaciones se aíslan respecto a otro tráfico que circula por la red evitando así problemas como retardo, latencia, congestión o pérdida de paquetes.

Se trata de un protocolo muy útil ya que es escalable a un gran número de aplicaciones y otorga un gran ahorro en costes; no es necesaria una gran cantidad de hardware debido a su completo desarrollo en la nube. De esta manera, MPLS permite a los operadores establecer conexiones VPN (*Virtual Private Network*), VPLS (*Virtual Private LAN Service*) y VLLS (*Virtual Leased Line*) en grandes redes públicas. Esta tecnología también se puede encontrar en grandes redes privadas.

Como desventaja principal, se destaca la carencia de seguridad en las comunicaciones.

2.2 *VPN (Virtual Private Network)*

Debido al aumento de la cantidad de usuarios remotos en las organizaciones y a la necesidad de acceso a sus redes centrales, existe una tendencia creciente hacia las redes seguras, trasparentes y productivas.

Para establecer una conexión de red privada extremo a extremo sobre una infraestructura pública, como Internet, las empresas utilizan VPN.

2.2.1 Definición

Una red virtual privada (VPN) es una red privada que, a través de enlaces virtuales, crea una conexión segura sobre otra red menos segura, como puede ser una red local tipo LAN.

Mecanismos como la encriptación permiten a usuarios VPN acceder de forma segura a redes situadas en distintas localizaciones. De esta manera, un equipo conectado a la red puede mandar y recibir información de redes públicas como si se tratara de una red privada con todos sus beneficios.

Su funcionamiento es simple, el tráfico viaja cifrado por túneles seguros completamente virtuales y los usuarios VPN, a través de métodos de autenticación -contraseñas u otro tipo de procesos de identificación- acceden al servidor VPN.

Mientras que, al comienzo, las VPN no constaban de sistemas de autenticación ni cifrado -eran simples túneles IP o enlaces virtuales punto a punto en nodos remotos- en la actualidad, su ventaja principal es la seguridad y la protección completa de los datos.

Controles de acceso, integridad, autorización o privacidad son algunos de los principales modelos de seguridad frente a usuarios no autorizados de la VPN. Esto la convierte en una red perfecta para aquellas organizaciones que deseen proteger sus datos.

No obstante, proveer seguridad a usuarios remotos o acceder a información no es el único propósito de estas redes. Las VPN son capaces de ocultar las actividades de búsqueda de los usuarios -lo que es particularmente útil por ejemplo en conexiones WiFi públicas- o permitir a estos la conexión a sedes bloqueadas geográficamente.

2.2.2 Tipos

Los tipos más comunes de redes VPN son:

2.2.2.1 VPN de Acceso Remoto:

Este tipo de VPN permite al usuario acceder a sus servicios y recursos de la red de manera dinámica. La conexión entre el usuario y la VPN se realiza mediante Internet de manera segura y privada. La seguridad en estas redes está garantizada gracias a métodos de encriptación.

Los clientes individuales son los principales usuarios de este tipo de VPN, pero también se utilizan en redes empresariales de ciertas organizaciones.

Un empleado, si se encuentra en un lugar geográfico diferente, puede conectarse de manera segura -mediante un dispositivo del servidor VPN próximo a la red- a la red de su compañía y acceder a los archivos y recursos.

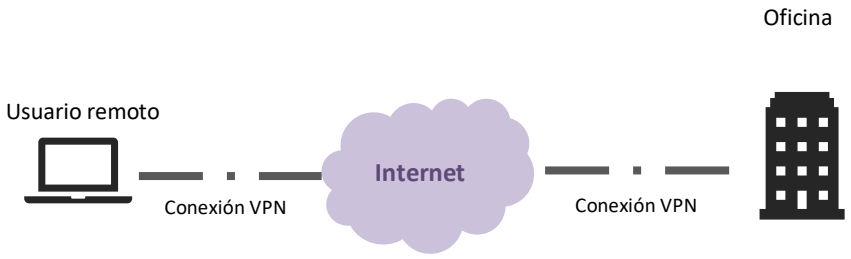


Figura 1. VPN de Acceso Remoto

En el caso de los usuarios privados de una VPN, estos disponen de un método de autenticación que les permite sobrepasar ciertas restricciones locales de Internet y acceder a contenido bloqueado. Los usuarios pueden además usar las VPN para mejorar la seguridad y la privacidad de sus datos en Internet.

La ventaja principal de estos accesos remotos es su facilidad de configuración, uso y accesibilidad -este tipo de VPN puede ser accesible fácilmente por cualquier tipo de usuario siempre que esté acompañado del software correcto.

2.2.2.2 VPN Sede a Sede

Las VPN Sede a Sede, también denominadas Router a Router, son generalmente usadas por grandes compañías. Estas organizaciones están formadas por oficinas de distintas localizaciones por lo que usan este tipo de VPN para interconectar las redes de las distintas oficinas entre sí.

Básicamente, se crea un túnel virtual entre las sedes y se establece una conexión permanente a Internet para que puedan mantener entre ellas una comunicación privada y segura. Un router actúa como cliente y otro como servidor y la comunicación comienza tras un método de autenticación.

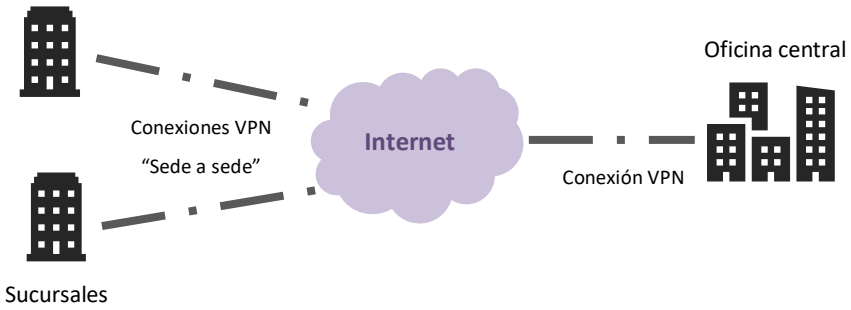


Figura 2. VPN Sede a Sede

Cuando múltiples oficinas de una misma compañía se interconectan usando redes VPN Sede a Sede se denomina Intranet. Se denomina Extranet cuando es necesario conectar dos Intranets separadas.

Este tipo de VPN son comunes en grandes compañías donde es crucial una comunicación segura entre departamentos de todo el mundo.

Debido a que las distintas redes se conectan mediante Internet, la contratación de otra red para el enlace cliente-servidor no es necesaria, lo que abarata los costes.

Su mayor desventaja es que son difíciles de implementar ya que requieren equipos especializados y grandes recursos. Además, esta tecnología, debido a que está desarrollada para un solo propósito, no ofrece flexibilidad.

2.2.3 Protocolos VPN

Un protocolo VPN determina exactamente cómo se direcciona la información entre un equipo y un servidor VPN. Los protocolos constan de diferentes especificaciones, ofreciendo a los usuarios beneficios como velocidad, privacidad o seguridad.

1- OpenVPN*:* este protocolo de código abierto es uno de los más seguros. Ofrece múltiples métodos de autenticación y está disponible para casi todas las plataformas.

2- PPTP *(Point-to-Point Tunneling Protocol):* debido a sus numerosas vulnerabilidades, *PPTP* se usa como último recurso cuando los demás protocolos fallan.

3- L2TP *(Layer 2 Tunneling Protocol):* mejor alternativa para dispositivos móviles que no son compatibles con *OpenVPN*. *L2TP* soluciona los puntos débiles de *PPTP*, pero aporta menor velocidad en sus accesos que *OpenVPN*.

4- IPSec *(Internet Protocol Security):* encripta los paquetes IP para su transporte, protegiendo así todo el tráfico de una red IP.

5- SSTP *(Secure Socket Tunneling Protocol):* encapsula tráfico VPN en sesiones HTTP.

6- IKEv2 *(Internet Key Exchange Protocol v2)*: crea sesiones para el intercambio de contraseñas.
IKEv2 se usa normalmente junto a IPSec en los modelos de encriptación y autenticación.

2.2.4 Beneficios

Como se ha comentado durante todo el apartado, este tipo de tecnología de red privada tiene grandes beneficios:

- La mayor ventaja de VPN es que es **más barata** que una red privada de área amplia (**WAN**) y en toda organización el objetivo es tratar con comunicaciones rentables.
- Las redes VPN evitan problemas de **escalabilidad** al hacer uso simplemente de las redes públicas. Particularmente para localizaciones internacionales y remotas, una VPN ofrece un alcance y una QoS (*Quality of Service*) mayor.
- La **seguridad** es el elemento principal de estas redes. Las VPN constan de un gran número de mecanismos para proteger nuestra **privacidad** y nuestros datos ante potenciales intrusos.
- Gracias a una VPN podemos acceder desde cualquier localización a nuestra información de manera **remota**, evitando así las restricciones existentes.

2.3 *MPLS VPN*

En MPLS VPN, una VPN consiste generalmente en un conjunto de sistemas remotos interconectados entre sí de manera segura gracias a una red MPLS central. Estos sistemas pueden ser de la misma organización o de distintas y, a su vez, todos los sistemas pueden estar conectados al mismo proveedor central de servicios o a diferentes.

Estas redes están basadas en un modelo P2P (*peer-to-peer*), lo que las hace más escalables y más fáciles de crear y manejar que las VPN convencionales. Asimismo, debido a la gran seguridad que ofrecen, las redes MPLS VPN son proveedoras de servicios como el alojamiento de datos, redes de comercio o telefonía.

El proveedor de servicios, en esta tecnología, utiliza el protocolo BGP (*Border Gateway Protocol*) para intercambiar con los nodos frontera -explicados en el punto *2.3.1.2*-, en cada VPN, las diferentes rutas; y MPLS para reenviar por el núcleo de la red la información de cada VPN, encapsulada con la etiqueta MPLS

correspondiente. Esto se realiza de manera que las rutas de las diferentes redes privadas se mantengan separadas.

El objetivo principal de este método es facilitar al cliente el uso de servicios centrales.

2.3.1 Arquitectura y Terminología

Los equipos que forman parte de una red MPLS tienen diferentes roles que son importantes para entender el funcionamiento de los servicios MPLS VPN. La diferencia entre estos equipos se basa principalmente en su localización dentro de la red y el tipo de conexiones, según sean P2P, circuitos virtuales ATM, túneles de nivel 2, interfaces Ethernet, etc.

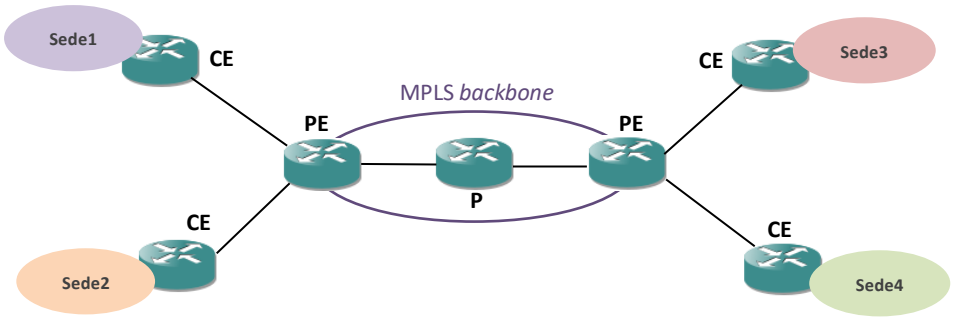


Figura 3. Tecnología MPLS VPN

2.3.1.1 P router (*Provider Router*)

Nodo interno parte del proveedor de servicios de la red MPLS y del camino del tráfico o LSP (*label-switched path*). Funciona como un nodo corriente de una red MPLS encargándose simplemente de conmutar etiquetas MPLS y mantener la señalización del tráfico. Nunca se conecta directamente con un nodo externo a la red ni conoce VPN.

2.3.1.2 PE router (*Provider Edge Router*)

Equipos situados en la frontera de la red MPLS, los cuales ofrecen interfaces a los clientes para su entrada en la red. Su función es clave ya que deben crear, para cada cliente, un servicio VPN dentro del núcleo MPLS. Son los únicos equipos que mantienen información sobre cada VPN en particular.

Mantienen separadas las tablas de rutas de la red MPLS y de los CE.

2.3.1.3 CE router (*Customer Edge Router*)

Estos dispositivos se encuentran en la frontera de la red del cliente. Están conectados a un equipo de la red local del cliente y a uno o varios PE, gracias a los cuales acceden a la red MPLS. Los CE, normalmente, utilizan dos protocolos de encaminamiento independientes en cada una de sus conexiones; un protocolo para intercambiar rutas con los equipos de la LAN y otro para intercambiar rutas con el PE. Estos CE no son conocedores de MPLS por lo que simplemente se encargan de enviar y recibir información e intercambiarla con el PE.

2.3.1.4 VRF (*Virtual Routing and Forwarding Table*)

Combinación de las tablas de direccionamiento y envío IP creadas para cada VPN en los PE.

VPN es un modelo p2p real que separa el tráfico asignando VRF únicas a cada cliente. De este modo, los usuarios de una VPN no son capaces de ver el tráfico externo a su red privada.

Cada VRF está asociada a un enlace PE-CE. Cuando en este enlace se recibe un paquete IP, el destino al que se debe dirigir el paquete se encuentra en la VRF del enlace. Si el enlace no está asociado a ninguna VRF, el destino lo determinará la tabla de direccionamiento por defecto.

En el caso de un enlace VRF sede-PE, el número de rutas que entran en la VRF correspondiente se puede limitar. La comunicación, vía equipos PE, está imposibilitada entre sedes que no tengan VPN común ya que las rutas asociadas se mantienen fuera de la tabla de direccionamiento.

En el caso de que una sede esté conectada a varios PE, en todas las VRF tiene que existir el mismo conjunto de rutas.

2.3.1.5 Sede

Concepto que se define como el conjunto de redes cliente conectadas al núcleo MPLS a través de una conexión PE-CE. Una sede puede formar parte de más de una VPN si es capaz de manejar rutas desde diferentes VPN. Asimismo, una VPN es un conjunto de sedes que comparte información común de encaminamiento.

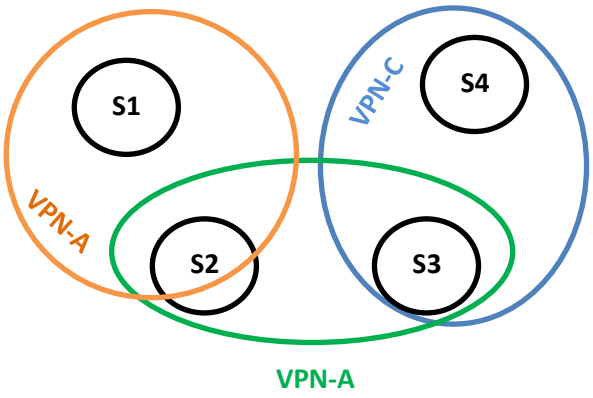


Figura 4. Sedes VPN

Una red privada o VPN no puede albergar sedes que usen el mismo rango de direcciones IP, ya que podría generarse una superposición de espacios de direccionamiento.

Cada sede debe contener uno o más equipos CE.

Cuando un PE está conectado al CE de una sede, se dice, de igual modo, que este PE está directamente conectado a la sede.

En este caso, la VRF estaría constituida por el conjunto de rutas disponibles para una sede o grupo de sedes conectados a un PE. Si existen varias sedes conectadas al mismo PE compartiendo la misma información de encaminamiento estos pueden situarse en una misma VRF.

En conclusión, generalmente, una sede consiste en un conjunto de sistemas geográficamente cercanos, incluso si cada uno consta de su propio CE. Una serie de sistemas IP con interconexión común sin red troncal puede considerarse una sede.

2.3.1.6 RD (*Route Distinguisher*)

Identificador numérico situado delante de la dirección IPv4, el cual la convierte en única dentro de un dominio MPLS. A este conjunto de doce bytes se le denomina dirección VPN-IPv4.

Este identificador permite a protocolos como BGP manejar rutas completamente distintas hacia una misma dirección usada en diferentes VPN. Análogamente, este identificador puede ser usado para crear múltiples rutas hacia un mismo sistema en el que se quiera, por ejemplo, diferenciar entre varios tipos de tráfico.

El propio PE debe ser el encargado de asociar el RD a las rutas direccionadas hacia un CE en particular.

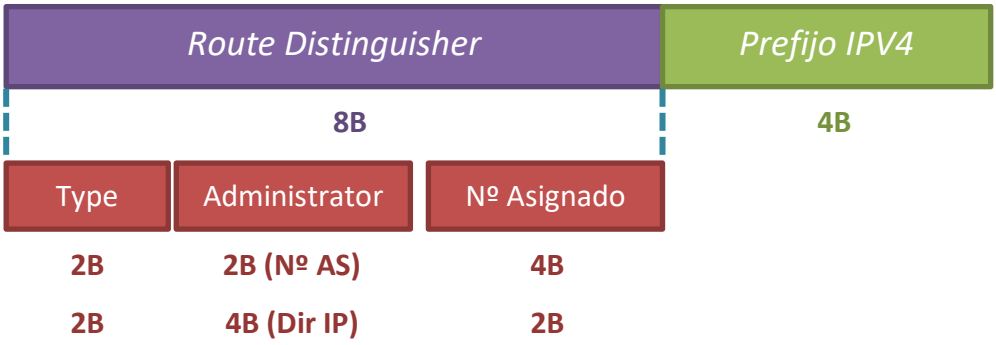


Figura 5. RD (Route Distinguisher)

2.3.1.7 RT (*Route Target*)

Atributo adicional de la tecnología MPLS VPN de Nivel 3 que le proporciona al PE la capacidad de saber qué rutas incluir en cada VRF. Cada VRF está ligada con uno o más RT.

Estos atributos pueden ser usados por un PE para determinar si las rutas recibidas deben ser incluidas en la VRF correspondiente. Los PE están configurados de manera que sepan qué RT asociar a cada ruta.

Su estructura es parecida a la de los RD.

2.3.1.8 RR (*Route Reflectors*)

Únicos sistemas que necesitan disponer de la información de enrutamiento de las VPN que no están directamente conectadas. Su existencia mejora la escalabilidad de la red.

Gracias a ellos, un nodo PE enlazado a una VPN en particular descubre automáticamente los otros PE conectados a esa misma VPN. De esta manera, cuando se añade un nuevo router o se produce un cambio en la topología, no se necesita una reconfiguración de los demás PE.

2.3.2 Ventajas

La mayor ventaja de esta tecnología es su alta escalabilidad. Debido a que la información de encaminamiento de cada VPN es guardada solo en el PE al que está conectado, al añadir una nueva sede solo serían necesarias las configuraciones de los nuevos routers PE y CE. Su escalabilidad se ve igualmente mejorada debido a que no son necesarias múltiples rutas, sino que una sola puede contener varios atributos, RT.

De igual manera, cada usuario tiene asignados en el PE sus propios RD y VRF ofreciendo así privacidad entre clientes. Esta información es intercambiada entre los distintos routers PE pertenecientes a una VPN sin comprometer a los routers P. Para ello, tanto el PE de entrada como el de salida deben ejecutar el mismo protocolo de encaminamiento.

La flexibilidad en los métodos de control de distribución de la información entre las distintas sedes es otra de sus grandes capacidades. Esto permite que la construcción de las VPN sea muy flexible.

2.3.3 Actividad

Como se ha comentado anteriormente, BGP es el protocolo usado en cada VPN para intercambiar información de encaminamiento entre los routers frontera PE.

Este protocolo hace posible el transporte de grandes cantidades de rutas y, como atributo opcional, de información adjunta a estas por lo que es perfecto para el manejo de rutas VPN y la propagación de RT entre los routers frontera.

2.3.3.1 Direccionamiento CE-PE y PE-CE

Los routers PE unidos a una VPN en particular necesitan conocer para cada enlace las direcciones a las que se puede llegar a través de él. La distribución de rutas en este enlace CE-PE puede realizarse mediante enrutamiento estático, RIP, OSPF o BGP.

Cuando un router PE recibe un paquete de su CE directamente conectado, debe determinar el circuito por el que el paquete ha llegado y por lo tanto la VRF que debe usarse para reenviar el paquete -normalmente, esta decisión se toma gracias a aspectos como la interfaz de llegada del paquete o su cabecera. [*2.3.3.2*]- De igual manera, este equipo PE aprende, de su CE, alguna de sus rutas VPN, las cuales pueden llegar a ser incluidas en la VRF vinculada a dicho circuito.

Estas rutas son convertidas por el PE en rutas VPN-IPv4, ligadas a uno o más RT -los cuales son llevados como atributos de la ruta- y posteriormente exportadas a BGP.

Si hay más de una ruta hacia la misma dirección, BGP escoge la mejor y la distribuye hacia los demás PE *[2.3.3.3]*. Cualquier ruta asociada con un RT debe ser distribuida hacia todo PE que disponga de una VRF vinculada a ese RT.

En resumen, la información de encaminamiento que le llega al PE de entrada, compuesta por las rutas VPN-IPv4 correspondientes con sus RT definidos en las VRF origen, es distribuida por BGP hasta el PE de salida.

El router PE de salida, al recibir las rutas gracias a BGP, escogerá de nuevo la mejor ruta hacia la dirección requerida. Las rutas recibidas se introducen en las tablas VRF basándose en los RT adjuntos. Cuando la ruta queda introducida en la VRF, el RD de la VPN-IPv4 se elimina obteniendo así de nuevo un encaminamiento IP habitual. Para finalizar, cualquier ruta obtenida

a través de BGP e incluida en una VRF es transmitida a los CE asociados. Cualquier proceso usado en la distribución de rutas CE-PE puede ser usado en las conexiones PE-CE.

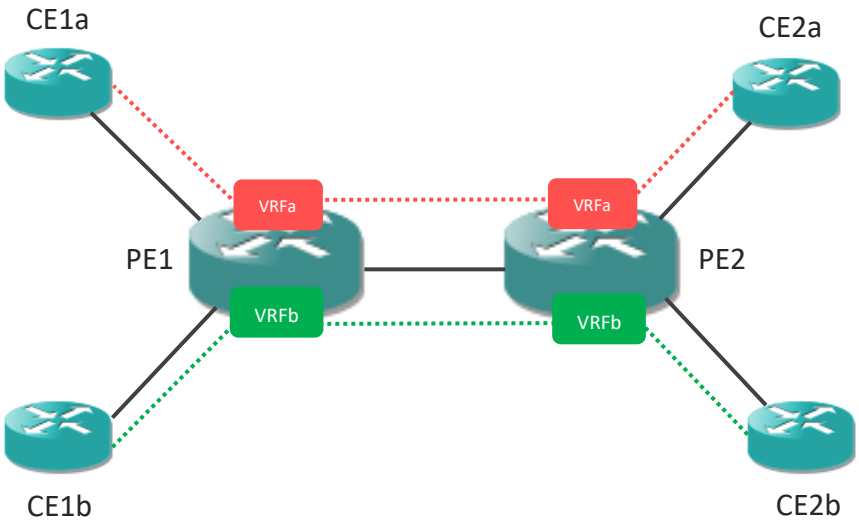


Figura 6. Direccionamiento VRFs

2.3.3.2 Reenvío en PE de entrada

Una vez que el PE sabe, gracias al circuito de entrada y la VRF, la dirección destino comienza el proceso de reenvío.

Primeramente, se conoce el primer salto del paquete:

- Si este salto no es alcanzable desde una VRF, el paquete debe realizar al menos un nuevo salto. A este paquete se le asignará una etiqueta MPLS para la mejor ruta destino y se convertirá entonces en un paquete MPLS con una etiqueta VPN en la pila.

- Si el circuito de entrada y de salida corresponden al mismo PE, pero están ligados a VRFs distintas, y la mejor ruta destino de la VRF de entrada es un conjunto de varias de la de salida, es necesario hacer igualmente una búsqueda de la dirección destino en la VRF de salida.

- Si este salto es directamente alcanzable, no es necesario insertar etiquetas MPLS en la pila y el paquete se envía con normalidad por el circuito de salida.

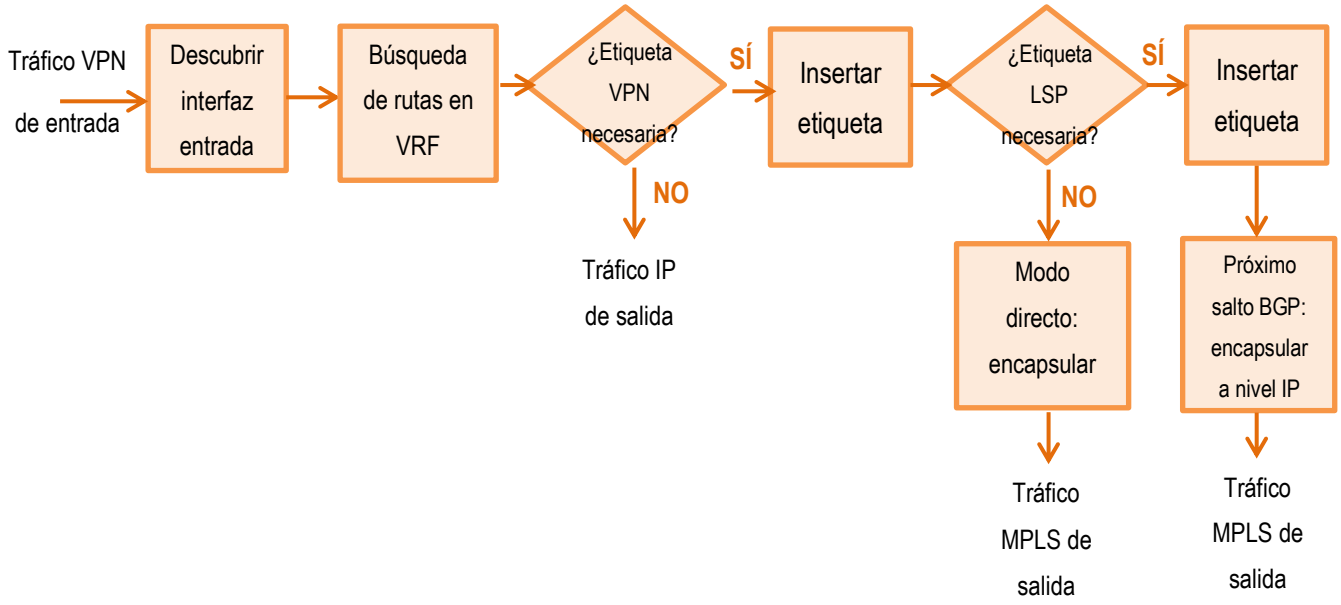


Figura 7. Reenvío de tráfico MPLS VPN

2.3.3.3 Distribución de rutas en el *backbone*

Cuando un PE distribuye por BGP una ruta VPN-IPv4, usa como siguiente salto su propia dirección. Si la red troncal soporta el protocolo MPLS, esta dirección se codifica con un RD igual a 0 y se le asigna una etiqueta MPLS, lo que la convierte en una ruta etiquetada VPN-IPv4.

Dos sedes de una VPN pueden intercambiar rutas VPN-IPv4 con varios PE gracias a un enlace iBGP si los PE pertenecen al mismo AS.

El PE receptor, tras el análisis del paquete obtenido, extrae la etiqueta de la ruta VPN y procesa el paquete con normalidad. Esta etiqueta puede dar información sobre la necesidad de búsqueda en la VRF, sobre el circuito de salida e incluso sobre su cabecera de enlace.

Puede darse la situación de tener una sola etiqueta para una VRF completa, una para cada circuito o una distinta para cada ruta.

En esta arquitectura VPN, debido al uso de MPLS, se debe tener en cuenta que el paquete MPLS que lleva la etiqueta debe ser enviado por un túnel que conecte el router BGP origen y el siguiente salto BGP. Este proceso requiere

de la existencia de un LSP entre los equipos, por lo que todos los sistemas deben soportar LDP (*Label Distribution Protocol*).

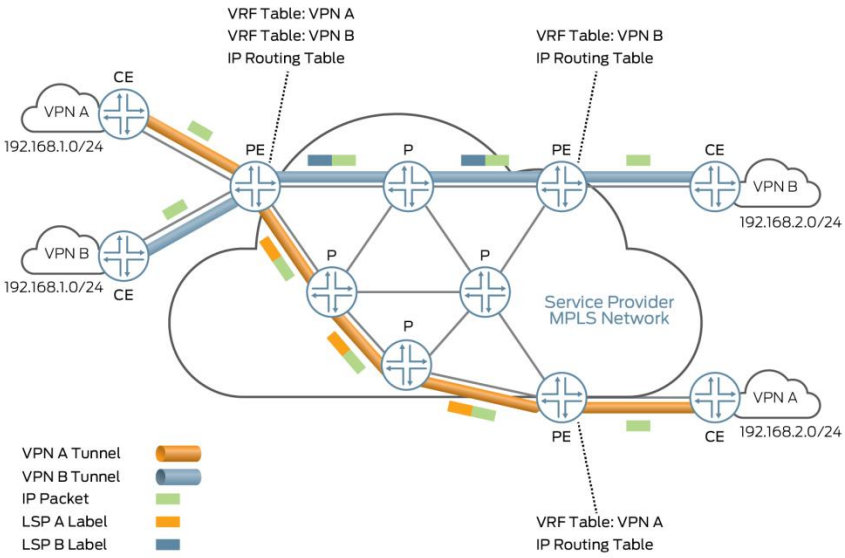


Figura 8. Túneles LSP [1]

Existen otros métodos MPLS como la presencia de túneles hacia el siguiente salto BGP. Si el paquete puede hacer uso de uno de estos túneles, se le asocia una etiqueta MPLS al túnel y se inserta en la pila de etiquetas. De esta forma, el paquete será enviado hacia el siguiente salto del túnel.

La tunelización de las etiquetas VPN por el *backbone* permite que los únicos equipos conocedores de ellas sean los PE. Esto ayuda, de igual manera, al aislamiento de las VPN, ya que los paquetes etiquetados que no pertenezcan a equipos de la red troncal no deben ser aceptados.

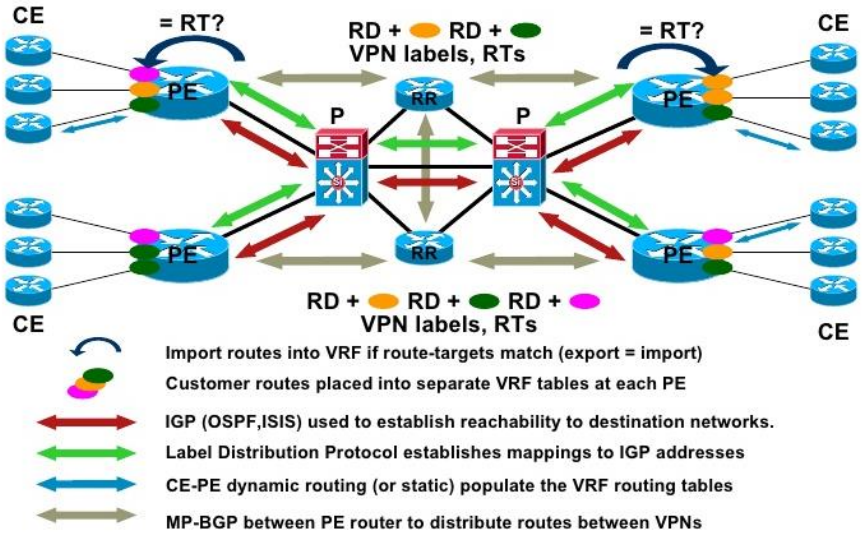


Figura 9. Funcionamiento completo MPLS VPN

2.4 VPLS (Virtual Private LAN Service)

En los últimos años ha emergido otra tecnología basada en MPLS. Las MPLS VPN de Nivel 2, también conocidas como VPLS, son, al igual que las de Nivel 3, un tipo de servicio VPN capaz de transportar tráfico IP y tráfico no IP haciendo uso de la misma infraestructura MPLS.

VPLS utiliza MPLS para crear la apariencia de una VPN en cada localización del cliente. Los paquetes Ethernet viajan por un túnel aislados del tráfico de otros usuarios de Internet. Las tramas son direccionadas según los estándares de Nivel 2 y la tolerancia a los fallos asegura que cada paquete llegue intacto a su destino.

Una red VPLS se parece en muchos aspectos a una LAN (*Local Area Network*), con la diferencia de que en VPLS los usuarios pueden estar distribuidos por un área amplia. Esta arquitectura tiene topología de malla por lo que puede ofrecer servicios p2p y multipunto. De hecho, VPLS tiene la capacidad, mediante un conmutador Ethernet virtualizado, de conectar múltiples LAN individuales como si funcionaran y formaran parte de una sola LAN.

Esta es el objetivo principal de VPLS, ofrecer conectividad entre sedes dispersadas geográficamente a través de MAN (*Metropolitan Area Network*) y WAN (*Wide Area Network*), como si estuvieran conectadas usando una LAN.

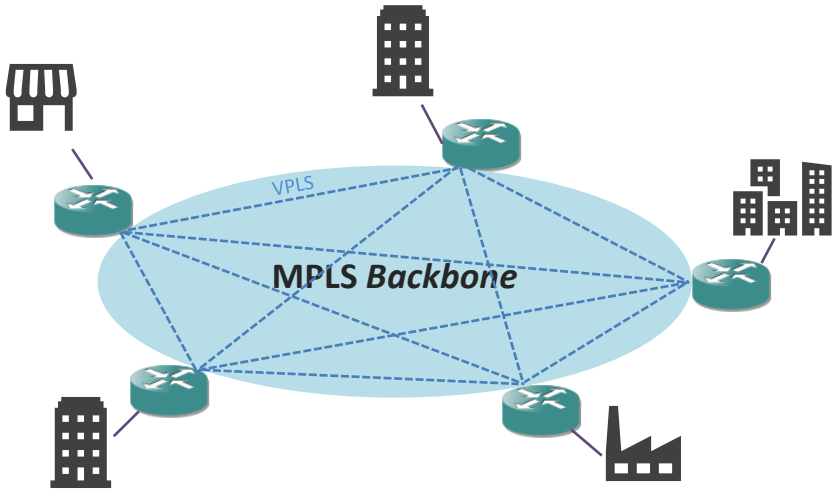


Figura 10. Red VPLS

Las LAN tradicionales proveen de los servicios *multicast* y *broadcast* necesarios para que las sedes pertenecientes al mismo dominio y conectadas gracias a una red MPLS direccionen el tráfico hacia el destino correspondiente. Sin embargo, nuevas funcionalidades como el aprendizaje de direcciones MAC o la réplica de paquetes para tráfico *multicast*/*broadcast* e inundaciones *unicast* también son necesarias.

VPLS se comporta como un gran conmutador con PE inteligentes en el aprendizaje de MAC. Y como en un conmutador, este aprendizaje se hace en el plano de reenvío.

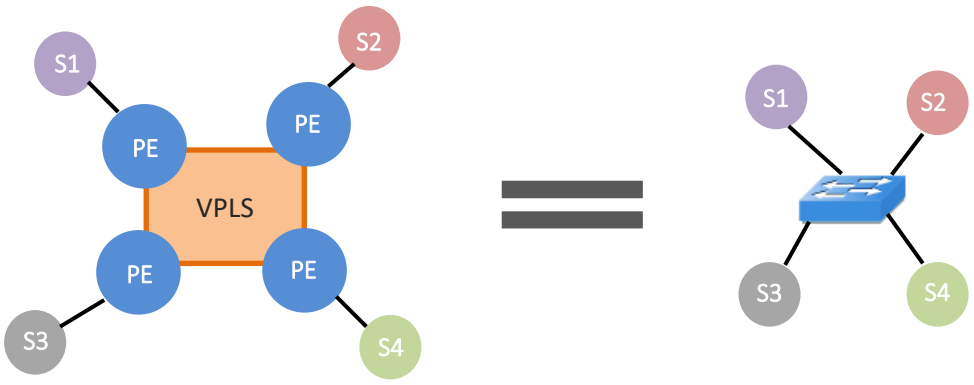


Figura 11. Conmutador VPLS

2.4.1 Arquitectura

La topología usada en esta arquitectura es parecida a la de las redes MPLS VPN, una red central MPLS formada por routers P (*Provider*) y PE (*Provider Edge*), y una red cliente con equipos CE (*Customer Edge*). Mientras que los PE conocen VPLS, los CE simplemente se conectan a otros CE mediante una red de conmutadores de Nivel 2. Estos conmutadores tampoco tratan VPLS.

2.4.1.1 PE routers

Este equipo dentro de una topología VPLS, tal como en una MPLS VPN, tiene dos conexiones clave, una hacia el núcleo MPLS y otra hacia el CE. De esta manera, se pretende brindar al cliente con una conexión Ethernet de Nivel 2 de forma transparente. No obstante, los planos de acceso y de red al realizar el control del tráfico de estos PE están muy diferenciados.

En el siguiente gráfico se muestran las diferencias en la pila de protocolos usada por el PE dependiendo del equipo al que esté conectado.

Conexión a nodo de red P	*Conexión a nodo cliente CE*
VPLS	
RSVP-TE	
LDP	
MPLS	
OSPF	
IP	
Protocolos Nivel 2: ETH, ATM, POS	Protocolos Nivel 2: ETH, ATM, POS
Nivel 1	Nivel 1

Tabla 4. Pila de protocolos de conexiones del PE

En un enlace PE-CE existe una relación entre la MAC del router CE y el puerto físico del PE. Esta relación facilita el aprendizaje de la localización del equipo.

Asimismo, debido a que este enlace se trata como transparente, el CE puede conectarse directamente al equipo remoto con el que quiera establecer comunicación sin llegar a escalar al nivel IP.

2.4.1.2 P routers

Al igual que en las redes MPLS VPN, estos routers P se encargan principalmente de la señalización del tráfico dentro del núcleo de la red -la pre-señalización del camino a seguir reduce el tiempo de conmutación. Sin embargo, debido a que estos equipos están sometidos al procesamiento de grandes cantidades de datos, para el correspondiente éxito del servicio a los clientes, también deben ser capaces de solucionar fallos tan comunes como cambios en la topología o caída de equipos y enlaces.

2.4.1.3 CE routers

La ventaja principal de estos equipos es que, debido a que por cada sede de cliente utilizan solo una dirección física, el tamaño de las MAC en la VPN del cliente se reduce.

2.4.2 Protocolos de señalización

VPLS, además de hacer uso del protocolo MPLS en su red central, establece un enlace entre los equipos PE de esta red mediante sesiones de señalización. Los protocolos BGP o LDP son los encargados de esta señalización.

En el caso de BGP (*Border Gateway Protocol*), se puede hacer uso de unas sesiones preexistentes entre los PE y de funcionalidades como la definición de instancias entre distintos proveedores o la autoconfiguración.

LDP (*Label Distribution Protocol*), sin embargo, es un protocolo menos escalable y flexible que maneja señalización p2p.

En la tecnología VPLS, para realizar la señalización, se puede configurar el protocolo BGP, LDP o ambos.

2.4.2.1 BGP (*Border Gateway Protocol*)

La auto-detección y la señalización son las funciones principales del plano de control de BGP. Estas dos funciones se realizan gracias a un solo mensaje de actualización BGP.

En el plano de datos se sitúan los métodos de encapsulación para el transporte Ethernet sobre MPLS y los de direccionamiento, como el aprendizaje de direcciones MAC o las inundaciones.

La configuración de estas redes es difícil debido a que los PE pertenecientes a una misma VPLS deben situarse en una topología tipo malla.

2.4.2.1.1 Auto-detección

En el proceso de auto-detección VPLS, los nodos frontera de la red detectan otros equipos PE que pertenezcan al mismo dominio VPLS gracias a un protocolo de señalización, en este caso BGP. Esto permite que la configuración de los PE se simplifique.

A través de la auto-detección también se detecta cuando otros PE son añadidos o eliminados del dominio. Por lo tanto, cuando esta funcionalidad está activa, al producirse algún cambio en la topología, no es necesaria ninguna configuración manual del dominio VPLS.

BGP hace uso del Nivel 2 de VPN para guardar la información de encaminamiento. Cuando BGP distribuye en los mensajes de actualización esta información hacia todos sus vecinos, la información es usada para configurar la topología de la red y que todos los equipos puedan soportar las funcionalidades de VPN Nivel 2.

2.4.2.1.2 Señalización

Una vez que la detección se ha realizado, debe empezar a realizarse la señalización. Cada par de PE debe ser capaz de establecer, y echar abajo, túneles entre ellos, así como de intercambiar información sobre estos.

Para estas redes VPLS es necesario hacer uso de un elemento como la etiqueta MPLS. La función de una etiqueta es la de diferenciar entre las distintas tramas de tráfico que circulan por un túnel. Sin embargo, en VPLS, esta etiqueta no se encarga solamente de tratar paquetes con diferente servicio, sino que también identifica el PE de entrada. El uso de etiquetas no implica que los túneles PE-PE se comporten como un túnel MPLS.

Todos los PE remotos necesitan esta etiqueta, por lo que el PE de entrada se encarga de enviar un mensaje de actualización común para todos el cual contiene un número de etiquetas igual al número de PE remotos que conforman la red.

Cada PE tiene un identificador propio único, por lo tanto, cuando un PE recibe el mensaje, observa la etiqueta común recibida por parte del emisor y añade su identificador único a la base de esta. De esta forma, cada PE receptor obtiene una etiqueta única de su PE emisor para esa instancia VPLS. Un PE puede guardar varios bloques de etiquetas.

Para establecer la conexión, el PE remoto debe comprobar si el emisor forma parte del conjunto de sus equipos remotos. Cuando se asegura, establece un túnel hacia el PE emisor. Este último comprueba si el PE final es alcanzable y establece otro túnel hacia él.

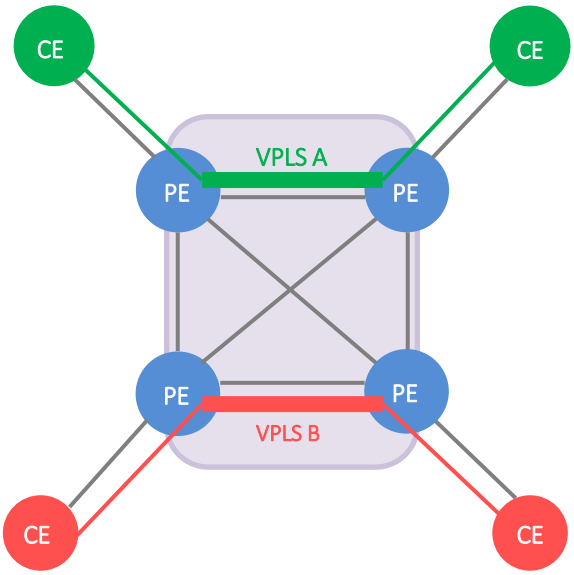


Figura 12. Túneles VPLS

2.4.2.1.3 Red VPLS Jerárquica

Las redes basadas en una tecnología VPLS, debido su topología de malla, tienen límite en su escalabilidad. El crecimiento del núcleo de estas redes puede ser difícil debido a la necesidad de un mallado completo con capacidad para manejar el tráfico de control de sus caminos.

Afortunadamente, el uso de BGP ha ofrecido soluciones para este problema. La técnica del plano de control más básica radica en la división de grandes redes en subredes o áreas -una jerarquía que sugiere distintos niveles para los equipos de la red. Estas áreas funcionan como servicios MPLS independientes, completamente malladas y con una sesión BGP entre cada nodo componente.

Se define un área central a la que estarán conectadas todas las áreas inmediatamente inferiores en jerarquía mediante uno o dos enlaces. Cada área inferior, cada vez que quiera enviar tráfico a otra, deberá mandarlo siempre a través del área central. De este modo, no es necesaria una conexión mallada completa entre todos los equipos BGP.

Esta técnica puede ser reproducida recursivamente. Si la red sigue aumentando su tamaño, más niveles de jerarquía deberán ser incluidos.

La división en jerarquías se sitúa completamente en el plano de control. El uso de estas subredes no entra en el plano de datos por lo que no produce ningún cambio en el camino del reenvío de tráfico VPLS.

2.4.2.2 LDP (*Label Distribution Protocol*)

LDP es el protocolo de señalización más extendido y más usado por los proveedores.

2.4.2.2.1 Señalización

Para establecer la correspondiente topología de mallas se usa una malla completa de sesiones LDP. Una vez que se ha creado la sesión entre dos PE, todos los PE entre estos son señalizados gracias a la misma sesión.

Para minimizar el tamaño de la red VPLS, se puede establecer una topología jerárquica.

2.4.2.2.2 Modelo Jerárquico

Al igual que en el modelo jerárquico de BGP, las redes se dividen en subredes o áreas y se define un área central o Core.

En este caso, todas las áreas están compuestas por equipos interconectados entre sí que se comunican mediante sesiones LDP e implementan una nueva funcionalidad llamada ***split-horizon***.

La regla *split-horizon* elimina el reenvío de información entre equipos de la misma área evitando así la formación de bucles en la red. Un PE no reenvía el tráfico por el mismo puerto por el que lo recibió, por lo que el mismo tráfico no es devuelto a su origen. Esta regla se aplica al propio túnel del cliente y a aquellas sesiones malladas LDP entre PE.

En este diseño, los caminos MPLS se definen mediante el protocolo RSVP-TE.

Cuando se aplica *split-horizon* sobre las mallas de cada área se evita que el mismo paquete le llegue a un mismo nodo por distintos caminos.

En esta arquitectura, no obstante, también es necesaria una conectividad con el área Core y con las demás áreas VPLS a las que el cliente esté conectado. La asociación ***spoke*** define una conexión LDP entre un área y el Core aplicando *split-horizon* en el enlace receptor del tráfico. De esta forma, el tráfico recibido por un enlace *spoke* con destino otra área se reenviará por todas las interfaces excepto por el que se ha recibido.

El Core tiene el mismo comportamiento que un área VPLS con su mallado completo LDP y libre de bucles. En este núcleo, solo aquellos equipos con conexiones *spoke* hacia otras áreas pueden reenviar el tráfico. Cuando el tráfico llega al área, el PE receptor se encarga de la **inundación** hacia las demás sesiones LDP.

- ***Inundación**: toda la red consta de réplicas de paquetes idénticas hasta que un equipo recibe una correctamente.*

Existe una topología redundante en la que se usan dos enlaces *spoke* hacia el Core en vez de una para evitar posibles fallas. Esta redundancia crea bucles lógicos que pueden ser solucionados con mecanismos de control como el *Rapid Spanning Tree Protocol*.

2.4.3 Aprendizaje de direcciones MAC

El aprendizaje consiste básicamente en asociar direcciones MAC origen de paquetes a la interfaz del equipo a la que llegan. Esta asociación se denomina *Forwarding Information Base* (FIB) y es usada para el reenvío de los paquetes. Una VPLS será consistente si todos los equipos de la red tienen la misma FIB, asegurando así que en todo momento se transmite un mínimo de información.

La primera vez que un equipo recibe un paquete en una de sus interfaces, crea una asociación MAC origen-interfaz. De esta manera, se consigue un vínculo entre el cliente generador del tráfico y un puerto físico. Si este equipo posteriormente recibe otro paquete con MAC destino igual a la MAC origen incluida anteriormente en la asociación, ya sabe que debe reenviar el paquete por esa interfaz. En el caso de que se reciba un paquete con la misma MAC origen en un puerto diferente, la FIB debe actualizarse. Las asociaciones deben actualizarse siempre que sucedan cambios en la topología.

Las FIB de un equipo constan de temporizadores que controlan el tiempo de cada asociación. Estas entradas pueden acabar siendo eliminadas si sobrepasan un cierto tiempo sin ser usadas.

El equipo de la red que recibe el tráfico reenvía el paquete por todos los puertos pertenecientes a la VPN excepto por el receptor. Este paquete, a su paso por los diferentes equipos de la red, va registrando asociaciones en las correspondientes FIB.

Al definirse todas estas asociaciones, cuando el equipo destino quiere reenviar el tráfico hacia el origen, su MAC se convierte en dirección origen y se reenvía de nuevo.

Cada vez que el nuevo paquete llega a uno de los equipos intermedios, gracias a la información de la FIB, se determina con facilidad el puerto de salida completando así en ese nodo el aprendizaje de la MAC para esa comunicación.

En esta segunda vez que se recibe el paquete, no se produce una inundación ya que todos los nodos son conocedores de la MAC a la que deben reenviar el paquete.

La comunicación se completa cuando el equipo inicial recibe la trama.

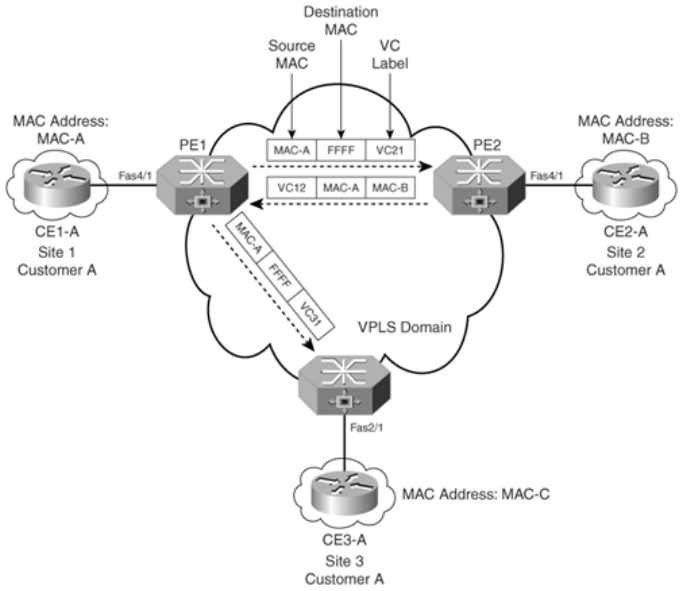


Figura 13. Aprendizaje de direcciones MAC [3]

En el caso de las redes VPN que hacen uso del protocolo LDP, la información de direccionamiento se obtiene gracias a funciones standard.

Cuando un paquete llega a un túnel, si la dirección MAC origen es desconocida, es necesario que esta se asocie al túnel para que el tráfico saliente hacia esa MAC pueda ser entregado a través del túnel asociado.

3. Análisis y diseño de la red

3.1 Planteamiento

En este apartado del estudio, se pretende diseñar y analizar las características de un ejemplo práctico de MPLS VPN que ilustre lo aprendido en el capítulo ***2***.

Los conceptos principales son:

- Las redes VPN permiten que varios clientes establezcan comunicación entre ellos mediante una red central MPLS o proveedor de servicios (SP). Un SP puede dar soporte a un gran número de VPN.

- Dentro de estas redes privadas, cada nodo usuario mantiene una VRF propia. Un equipo cliente solo puede mandar paquetes a otro nodo que tenga igual VRF.

3.2 Desarrollo del diseño

Como se puede observar, en estas redes existen dos partes diferenciadas, una red central o SP y una red cliente formada por varias VPN. Por ello, se ha decidido implementar dos topologías diferentes, una que aporte mayor conocimiento sobre el funcionamiento del *backbone* y otra, sobre las VPN. Ambas corresponderán a la tecnología MPLS VPN.

La primera topología, y más básica, se definirá en este apartado mientras que la segunda será desarrollada como una de las cuestiones del enunciado de la práctica final propuesta más adelante, en el apartado *5*.

3.2.1 Dimensionamiento

3.2.1.1 Red central

La red central deberá estar compuesta por un mallado adecuado que soporte grandes cantidades de tráfico.

Para estas redes MPLS se pueden considerar dos topologías de red:

- *Full mesh:* interconexión entre todos los nodos de la red sin pasar por un equipo central.

- *Hub and spoke:* todo el tráfico de los clientes pasa por un nodo central.

Generalmente, por razones obvias de seguridad, la opción escogida es la de *full mesh*. Sin embargo, en este caso, considerando que todas las características del protocolo MPLS se han estudiado previamente y que el objetivo principal actual es la tecnología MPLS VPN, se ha preferido hacer uso de una topología *Hub and Spoke*. Debido a que los recursos de la red no serán muy grandes no se observarán problemas de congestión. Asimismo, al ser una red con una topología simple, no existe gran dificultad ante la posibilidad de aumentar el número de equipos.

La red central de esta primera topología se compone de cinco equipos. Esto nos permitirá observar los intercambios de etiquetas MPLS que se producen en los diferentes saltos del camino.

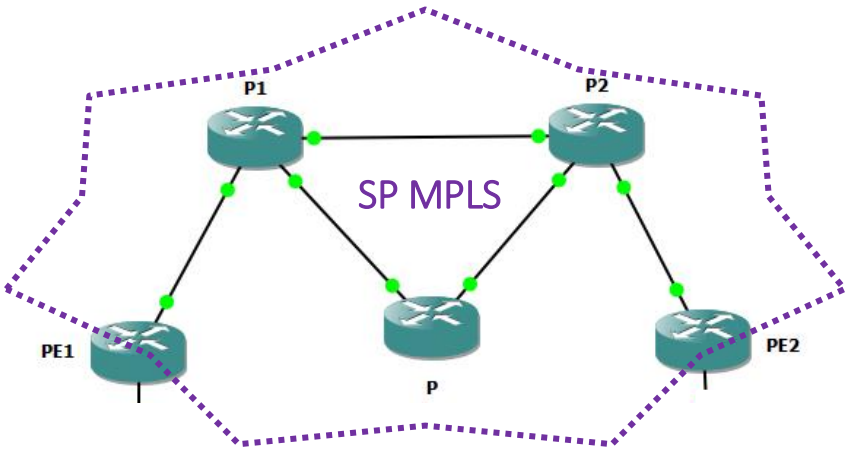


Figura 14. Backbone topología 1

3.2.1.2 Red cliente

Dos simples conexiones CE-PE son las encargadas de formar esta red.

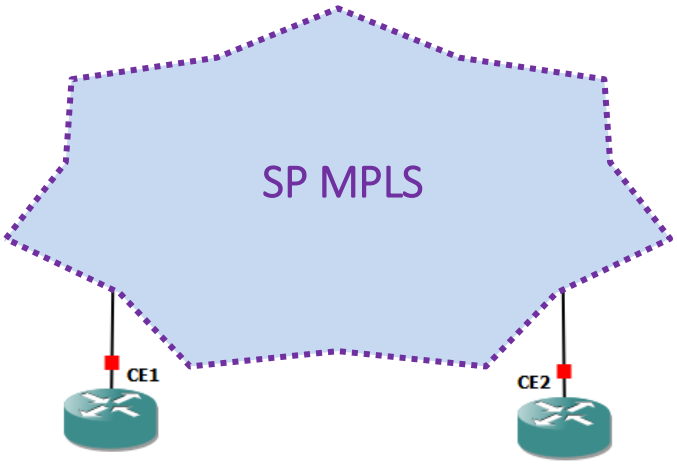


Figura 15. Red cliente topología 1

3.2.2 Definición y elección de *routing*

En este punto se deciden los protocolos de *routing* a usar en cada red, así como otras características de la red.

3.2.2.1 Red central

Para esta topología, se escoge un IGP que ofrezca tiempos de convergencia menores y sepa actuar ante los posibles bucles, uno de tipo Estado-Enlace.

Dentro de este grupo de protocolos, ya que no se prevé un gran crecimiento de la red, se elige OSPF. Además de ofrecer facilidad en su configuración, nos permite tener varios procesos activos, uno por interfaz, en el mismo router.

El número que identifica el proceso OSPF de la red central, local para cada nodo, es el 1. Asimismo, el área 0 será la configurada en la totalidad de la topología.

El identificador de router de cada proceso OSPF será igual a la dirección de su interfaz *Loopback0*.

Los cinco nodos que forman esta red, además de usar OSPF, también entienden MPLS y su correspondiente LDP para las operaciones de distribución de etiquetas.

3.2.2.2 Red cliente

Primeramente, para anunciar los prefijos de las VPN en la red es necesario hacer uso de una extensión de BGP denominada MP-BGP. Un equipo PE envía el paquete que contiene la etiqueta MPLS con el prefijo VPN y MP-BGP se encarga de anunciarla al otro PE de salida.

Solo los equipos PE implementan BGP. Para esta sesión BGP se define simplemente el Sistema Autónomo 1, el cual será igual para toda la red creando así un punto de estabilidad.

En el caso de la conexión CE-PE, se configura un número de proceso OSPF diferente por cada VRF. Los CE tienen, como los demás nodos de la topología, definidos localmente el proceso OSPF 1.

Aunque BGP es el protocolo más efectivo en este tipo de conexiones, en estos enlaces CE-PE usamos OSPF debido a que en BGP tanto la diferenciación del tráfico entre Sistemas Autónomos iguales como la redistribución final son más complejas.

La ilustración final de la topología con la definición de sus protocolos se encuentra en el punto *3.5*.

3.3 *Designación de los equipos*

Para la implementación de esta práctica se ha decidido usar routers Cisco 3600 para la parte cliente y routers Cisco 7200 para componer el *backbone*.

3.3.1 C7200

La serie de equipos de la familia c7200 se caracteriza por ofrecer una amplia gama de funcionalidades acompañadas de un gran comportamiento, escalabilidad, modularidad y precio.

Su arquitectura depende principalmente de la combinación de tarjetas procesadoras (NPE) y del *chassis*. Según esta combinación se pueden diferenciar

entre routers con plano medio original y routers con plano medio VXR. Los C7200 VXR pueden llegar a ofrecer hasta 1 Mbps.

En este caso, la IOS soportada por GNS3 es la del modelo C7206 VXR con NPE-400 (400 kpps).

Figura 16. c7206/NPE-400 [4]

Este equipo consta de controlador I/O, adaptadores de puertos y de servicios, tarjeta procesadora, fuente de alimentación, consola y cables auxiliares.

Algunas de las características del equipo son:

- La NPE-400 usa SDRAM para guardar todos los paquetes recibidos o enviados por las interfaces. Además, su memoria caché tiene tres niveles, dos internos al microprocesador y uno externo de 4MB que ofrece almacenamiento de alta velocidad para datos e instrucciones.

- Sus opciones de conectividad son: Gigabit Ethernet, Fast Ethernet 100BASE-TX, Ethernet 10BASE-T, Packet Over Sonet (POS), ATM y Token Ring (full y half duplex).

- Algunos de los protocolos soportados son ARP, IP Multicast, TFTP, UDP, MPLS, VLAN, EIGRP, IGRP, IS-IS, BGP, OSPF, RIP, ICMP, IPv6, SNMP…

- Las funcionalidades claves incluyen QoS (baja latencia, RED, policing, marking, shaping…), MPLS (MPLS VPN, MPLS TE, MPLS Qos), agregación de ancho de banda (PPP, IP-to-IP Voice, LFI, RBE…) y Tunneling (GRE, L2TP, UTI…).

Como se puede ver, esta familia de *routers* soporta una gran cantidad de funcionalidades, sobre todo respecto a MPLS, por ello se ha decidido implementar con ellos la parte de la red central. Otras opciones podrían ser las series c2691 o c3640.

3.3.2 C3660

En el caso de los equipos cliente, CE, estos pueden ser cualquier router que pueda establecer comunicación con su nodo frontera, PE, directamente conectado.

La serie c3600 permiten conexión de marcado, *routing* LAN-to-LAN, optimización de redes WAN e integración multi servicio de voz, vídeo y datos.

Esta vez, la IOS soportada por GNS3 es la del equipo c3660 IP PLUS IPSec 3DES.

Figura 17. c3660 [5]

El c3660 tiene seis módulos libres, los cuales aceptan una gran variedad de tarjetas de interfaz de red incluyendo tarjetas LAN y WAN que soportan tecnologías Fast Ethernet, Ethernet, Token Ring y variedades de WAN. Igualmente, este equipo consta de otros dos módulos internos libres para integración avanzada (AIM) y uno o dos puertos para Fast Ethernet 100BASE-TX.

El AIM reduce los costes recurrentes de la WAN y maximiza el beneficio de la administración de ancho de banda. Estos módulos internos extra permiten,

además, que los módulos externos queden disponibles para otros componentes como ATM, voz, *modems* analógicos y digitales, CSUs, etc.

IPSec 3DES es una funcionalidad añadida de estos routers por la cual se obtienen métodos de seguridad en la red como confidencialidad, integridad y autenticación de datos. Crea así túneles seguros entre equipos lo que aumentará la calidad de las VPN de estas topologías.

3.4 Simulación en GNS3

En este proyecto se van a definir, como se ha indicado anteriormente, dos topologías distintas. La primera topología se muestra en este apartado.

Contamos con la topología MPLS VPN siguiente:

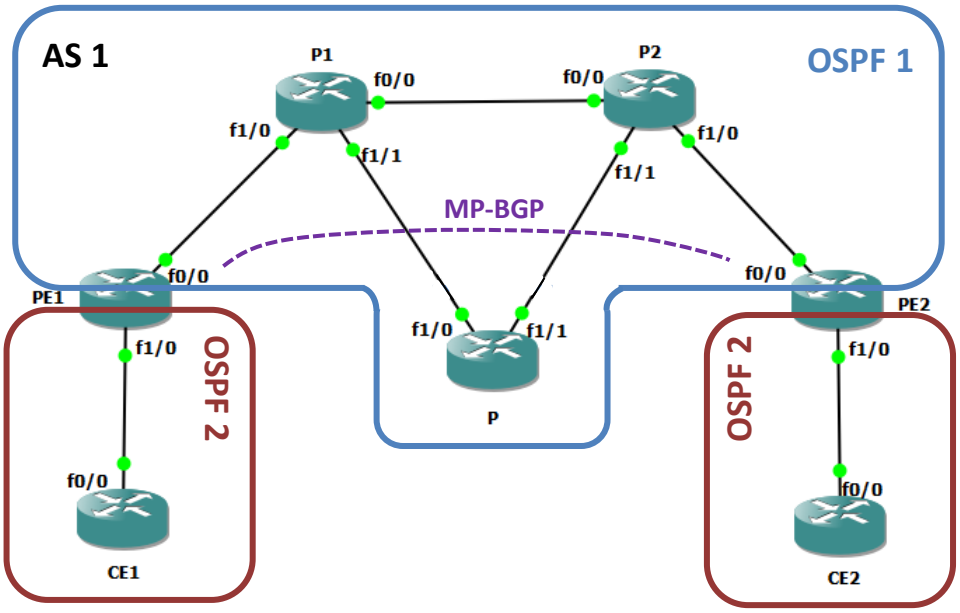


Figura 18. Protocolos topología 1

Como se puede observar, esta topología está compuesta por:

- P (*provider*): tres equipos situados en el núcleo que no tienen comunicación con el cliente.
- PE (*provider edge*): nodos frontera que permiten la comunicación entre las redes VPN y la red troncal.

- CE (*customer edge*): routers cliente

Teniendo claros estos conceptos ya podemos comenzar con la configuración.

3.4.1 Desarrollo

El desarrollo de estas redes MPLS VPN se basa en siete pasos:

a- *Configurar rutas estáticas*

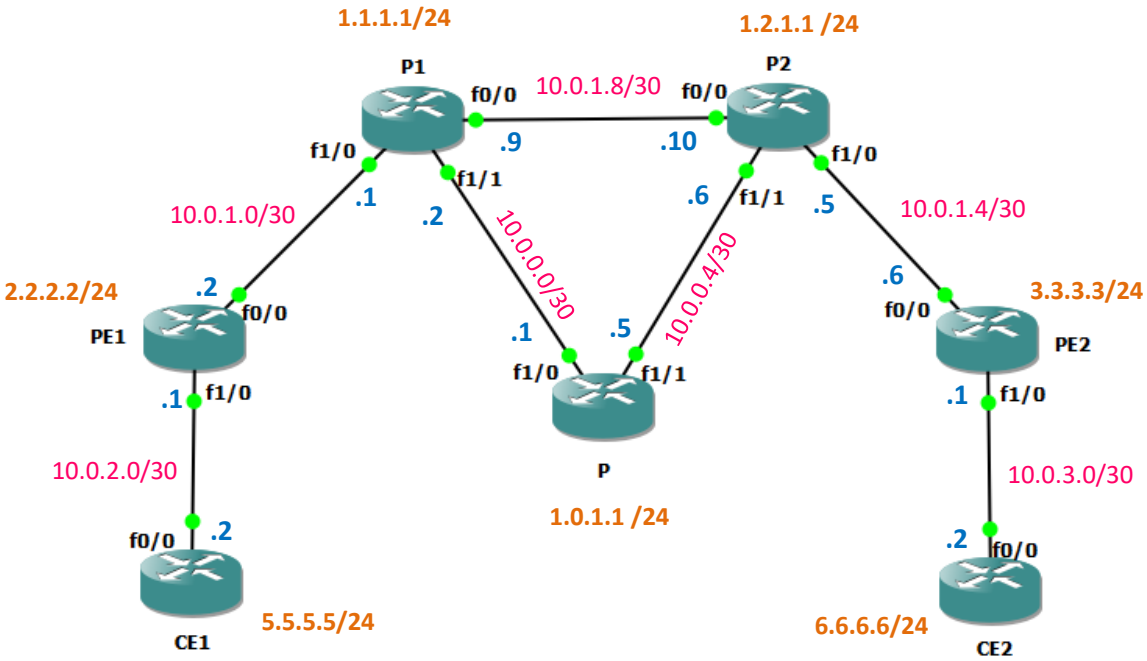


Figura 19. Rutas topología 1

P

```
interface Loopback0
 ip address 1.0.1.1 255.255.255.0
!
interface FastEthernet1/1
 ip address 10.0.0.5 255.255.255.252
!
interface FastEthernet1/0
 ip address 10.0.0.1 255.255.255.252
 !
```

P1

```
interface Loopback0
 ip address 1.1.1.1 255.255.255.0
!
interface FastEthernet1/1
 ip address 10.0.0.2 255.255.255.252
!
interface FastEthernet1/0
 ip address 10.0.1.1 255.255.255.252
 !
interface FastEthernet0/0
 ip address 10.0.1.9 255.255.255.252
 !
```

P2

```
interface Loopback0
 ip address 1.2.1.1 255.255.255.0
!
interface FastEthernet1/1
 ip address 10.0.0.6 255.255.255.252
!
interface FastEthernet1/0
 ip address 10.0.1.5 255.255.255.252
!
interface FastEthernet0/0
 ip address 10.0.1.10 255.255.255.252
!
```

PE1

```
interface Loopback0
 ip address 2.2.2.2 255.255.255.0
!

interface FastEthernet0/0
 ip address 10.0.1.2 255.255.255.252
!
```

```
interface FastEthernet1/0
 ip address 10.0.2.1 255.255.255.252
 speed auto
 duplex auto
!
interface FastEthernet1/1
  no ip address
  shutdown
  duplex full
!
```

PE2

```
interface Loopback0
 ip address 3.3.3.3 255.255.255.0
!

interface FastEthernet0/0
 ip address 10.0.1.6 255.255.255.252
 !
interface FastEthernet1/0
 ip address 10.0.3.1 255.255.255.252
 speed auto
 duplex auto
 !
interface FastEthernet1/1
  no ip address
  shutdown
  duplex full
!
```

CE1

```
interface Loopback0
 ip address 5.5.5.5 255.255.255.0
!
interface FastEthernet0/0
 ip address 10.0.2.2 255.255.255.252
 duplex auto
 speed auto
```

CE2

```
interface Loopback0
 ip address 6.6.6.6 255.255.255.0
!
interface FastEthernet0/0
 ip address 10.0.3.2 255.255.255.252
 duplex auto
 speed auto
!
```

- `Duplex full`: los datos pueden transmitirse simultáneamente en ambas direcciones. Por defecto.
- `Duplex auto & speed auto`: el algoritmo de auto-negociación permite a dos equipos anunciar y negociar el modo operacional del enlace. En este caso, se trata la velocidad y el tipo de duplex, *half* o *full*, del link.

b- *Activar OSPF en la red central*

Dado que ya existe conectividad IP, puede establecerse el protocolo de enrutamiento. En este caso se define OSPF para anunciar todas las interfaces *loopback* de la red proveedora de servicios.

En P, P1, P2, PE1 y PE2, la configuración de un protocolo de enrutamiento tiene mayor importancia ya que posteriormente, al activar MPLS, LDP hará uso de las direcciones *loopback* de vecinos no conectados directamente como direcciones de transporte para las conexiones TCP.

LDP es el protocolo de enrutamiento usado para la distribución de etiquetas MPLS entre los nodos de la red central.

En el caso de PE1 y PE2 en este apartado solo se configurarán las redes OSPF de las interfaces que pertenecen a la red central.

P

```
router ospf 1
 router-id 1.0.1.1
```

```
 network 1.0.1.0 0.0.0.255 area 0
 network 10.0.0.0 0.0.0.3 area 0
 network 10.0.0.4 0.0.0.3 area 0
```

P1

```
router ospf 1
 router-id 1.1.1.1
 network 1.1.1.0 0.0.0.255 area 0
 network 10.0.0.0 0.0.0.3 area 0
 network 10.0.1.0 0.0.0.3 area 0
 network 10.0.1.8 0.0.0.3 area 0
```

P2

```
router ospf 1
 router-id 1.2.1.1
 network 1.2.1.0 0.0.0.255 area 0
 network 10.0.0.4 0.0.0.3 area 0
 network 10.0.1.4 0.0.0.3 area 0
 network 10.0.1.8 0.0.0.3 area 0
```

PE1

```
interface Loopback0
 ip ospf network point-to-point
!
router ospf 1
 router-id 2.2.2.2
 network 2.2.2.0 0.0.0.255 area 0
 network 10.0.1.0 0.0.0.3 area 0
```

PE2

```
interface Loopback0
```
//Por defecto la ruta hacia una loopback es anunciada como la más específica (prefijo /32) ignorando el prefijo configurado. Para impedirlo hay que establecer p2p como el tipo de red:
```
 ip ospf network point-to-point
!
router ospf 1
```

```
 router-id 3.3.3.3
 network 3.3.3.0 0.0.0.255 area 0
 network 10.0.1.4 0.0.0.3 area 0
```

c- *Activar MPLS en la red central*

Una vez que la topología tiene ya su enrutamiento dinámico, se debe activar MPLS en los equipos que pertenecen al SP. LDP se activa automáticamente como protocolo por defecto.

Los equipos P envían tráfico solamente gracias a MPLS y el IGP correspondiente por lo que su configuración culmina aquí.

```
P(config)# interface f1/0
//comando para activar MPLS en una interfaz:
P(config-if)# mpls ip
P(config)# interface f1/1
P(config-if)# mpls ip

P1(config)# interface f0/0
P1(config-if)# mpls ip
P1(config)# interface f1/0
P1(config-if)# mpls ip
P1(config)# interface f1/1
P1(config-if)# mpls ip

P2(config)# interface f0/0
P2(config-if)# mpls ip
P2(config)# interface f1/0
P2(config-if)# mpls ip
P2(config)# interface f1/1
P2(config-if)# mpls ip

PE2(config)# interface f0/0
PE2(config-if)# mpls ip

PE1(config)# interface f0/0
PE1(config-if)# mpls ip
```

Los equipos cliente no hacen uso de MPLS.

d- *Creación de VRFs y asignación de interfaces*

El siguiente paso es crear las VRF en los nodos frontera para habilitar así el reenvío de las VPN. Para ello, se necesita asignar un RD único y uno o más RT a cada VRF.

En este caso solo se va a definir una VRF denominada *userA*. Los CE no conocen ninguna ruta fuera de su VRF.

```
PE1(config)#ip vrf userA
PE1(config-vrf)#rd ?
  ASN:nn or IP-address:nn  VPN Route Distinguisher
```

// route distinguisher usado en la forma <ASN>:<num_cliente>

```
PE1(config-vrf)# rd 1:1
```

Las rutas de las VRF distribuidas hacia el otro nodo frontera a través del SP son indicadas mediante los RT.

// route-target both es un comando que engloba los comandos route-target export y route-target import. Se encargan de la importación y exportación de RTs en la VRF. En este caso, estos procesos se realizarán hacia el AS definido, AS 1.

```
PE1(config-vrf)# route-target both 1:1
```

```
PE1#show run | begin vrf
ip vrf userA
 rd 1:1
 route-target export 1:1
 route-target import 1:1
```

```
PE2(config)# ip vrf userA
PE2(config-vrf)# rd 1:1
PE2(config-vrf)# route-target both 1:1
```

Una vez que se han definido las VRF, se les debe asociar las interfaces correspondientes:

```
PE1(config)# interface f1/0
PE1(config-if)# ip vrf forwarding userA

PE2(config)# interface f1/0
PE2(config-if)# ip vrf forwarding userA
```

e- *Configurar BGP en los nodos frontera*

Para que las rutas VRF y VPN puedan ser anunciadas entre PE, es necesario configurar una extensión de BGP para direcciones múltiples llamada MP-BGP.

El proceso comienza con la activación de BGP en el nodo. Posteriormente, se configura el equipo con el que intercambiará los paquetes y por último se indicará la dirección *Loopback0* como origen de actualizaciones BGP.

PE1

```
//Habilitar BGP en el router para el AS 1 del backbone:
router bgp 1
 bgp log-neighbor-changes

//Creación de entrada para el vecino interno al AS local en la tabla de vecinos BGP:
 neighbor 3.3.3.3 remote-as 1

//Uso de dirección IP específica al intercambiar mensajes de actualización con otro router:
 neighbor 3.3.3.3 update-source Loopback0
 !
 address-family vpnv4
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community extended
```

PE2

```
router bgp 1
 bgp log-neighbor-changes
 neighbor 2.2.2.2 remote-as 1
 neighbor 2.2.2.2 update-source Loopback0
 !
 address-family vpnv4
  neighbor 2.2.2.2 activate
//Solo se enviarán atributos extended al vecino
  neighbor 2.2.2.2 send-community extended
```

f- Configurar OSPF en los enlaces PE-CE

En este caso, en la conexión PE-CE se va a usar, como IGP, OSPF.

CE1

```
interface Loopback0
 ip ospf network point-to-point
 ip ospf 1 area 0
!
interface FastEthernet0/0
 ip ospf 1 area 0
!
router ospf 1
 router-id 5.5.5.5
 log-adjacency-changes
 network 10.0.2.0 0.0.0.3 area 0
```

CE2

```
interface Loopback0
 ip ospf network point-to-point
 ip ospf 1 area 0
!
interface FastEthernet0/0
 ip ospf 1 area 0
!
router ospf 1
 router-id 6.6.6.6
```

```
 network 10.0.3.0 0.0.0.3 area 0
 log-adjacency-changes
```

Los equipos CE ya tienen su configuración como proceso OSPF 1 de un solo área, área 0.

En el caso de los PE, para tener diferenciadas las dos redes principales de esta topología, se define para este enlace un nuevo proceso OSPF 2.

PE1

```
interface FastEthernet1/0
 ip ospf 2 area 0
¡
router ospf 2 vrf userA
 router-id 10.0.2.1
 net 10.0.2.0 0.0.0.3 area 0
//Cuando un router OSPF se configura como VRF-Lite se cree conectado al SP MPLS. Debido a que piensa que pertenece a esta red, no instala LSAs tipo 3 por lo que no hay prevención contra bucles. Para deshabilitar esta cualidad y que el nodo pueda usar los LSAs tipo 3 aprendidos del SP se usa:
 capability vrf-lite
```

PE2

```
interface FastEthernet1/0
 ip ospf 2 area 0
¡
router ospf 2 vrf userA
  router-id 10.0.3.1
  net 10.0.3.0 0.0.0.3 area 0
  capability vrf-lite
```

g- *Redistribución entre red cliente y red central*

Con la topología configurada casi en su totalidad, nos podemos fijar en la diferencia entre los enlaces MPLS y BGP de la red central y el direccionamiento de las rutas VPN desde los CE en la red cliente.

Para que estas redes tan diferentes puedan establecer comunicación es necesario configurar un proceso de redistribución de rutas en los nodos frontera.

```
// Redistribución de BGP en los procesos OSPF de lo CEs:
PE1(config)# router ospf 2 vrf userA
PE1(config-router)# redistribute bgp 1 subnets
// Redistribución de las rutas OSPF de los CEs en cada VRF hacia
BGP:
PE1(config)# router bgp 1
PE1(config-router)# address-family ipv4 vrf userA
PE1(config-router-af)# redistribute ospf 2

PE2(config)# router ospf 2 vrf userA
PE2(config-router)# redistribute bgp 1 subnets
PE2(config)# router bgp 1
PE2(config-router)# address-family ipv4 vrf userA
PE2(config-router-af)# redistribute ospf 2
```

Finalmente, la topología está configurada en su totalidad. Para cerciorarnos de que todos los procesos funcionan de manera correcta deben realizarse varias pruebas.

3.4.2 Análisis de pruebas

Correspondiéndose con el apartado ***3.4.1***, el análisis de pruebas también se dividirá en los mismos pasos -no se incluyen los test de los pasos *a* y *b* ya que no aportan pruebas suficientes sobre el correcto funcionamiento de una tecnología MPLS VPN.

Las comprobaciones se realizarán en el equipo PE1. No obstante, en algunos casos en los que otros equipos ofrezcan datos de mayor precisión, las pruebas se ejecutarán en estos últimos. En dichas ocasiones, se especificará el equipo a evaluar.

c- *Activar MPLS en la red central*

Una vez que tanto OSPF como MPLS están activados en la red central, la activación de LDP en las correspondientes interfaces es notificada, así como el anuncio de sus vecinos LDP.

%LDP-5-INFO: FastEthernet0/0: LDP started

%OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on FastEthernet0/0 from LOADING to FULL, Loading Done

%LDP-5-NBRCHG: LDP Neighbor 1.1.1.1:0 (1) is UP

Gracias a los comandos `show mpls interfaces` y `show mpls ldp neighbor` se pueden observar cuáles son los vecinos LDP con sus direcciones, las conexiones TCP y otra información de interés.

```
PE1#show mpls interfaces
Interface              IP            Tunnel   BGP Static Operational
FastEthernet0/0        Yes (ldp)     No       No  No     Yes
```

```
PE1#show mpls ldp neighbor
    Peer LDP Ident: 1.1.1.1:0; Local LDP Ident 2.2.2.2:0
        TCP connection: 1.1.1.1.646 - 2.2.2.2.36543
        State: Oper; Msgs sent/rcvd: 12/12; Downstream
        Up time: 00:00:10
        LDP discovery sources:
          FastEthernet0/0, Src IP addr: 10.0.1.1
        Addresses bound to peer LDP Ident:
          10.0.1.9        10.0.1.1        10.0.0.2        1.1.1.1
```

d- *Creación de VRF y asignación de interfaces*

```
PE1#show ip vrf interfaces
Interface              IP-Address      VRF                              Protocol
Fa1/0                  10.0.2.1        userA                            up
```

En este paso, se puede observar también la activación de las VRF en cada interfaz. Su correcto funcionamiento se muestra al hacer un `ping` desde el nodo frontera hacia el equipo cliente.

```
PE1# ping vrf userA 10.0.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 68/95/120 ms
```

e- *Configurar BGP en los nodos frontera*

Una sesión BGP entre los PE ha sido creada por lo que ahora estos equipos se reconocen como vecinos. Cuando se configura BGP en ambos equipos se puede observar su activación:

```
%BGP-5-ADJCHANGE: neighbor 3.3.3.3 Up
```

En el caso de que se quiera obtener más información sobre la sesión BGP, el comando `show bgp vpnv4 unicast all summary` ofrece datos de gran interés. En este punto no existen rutas en la tabla BGP ya que no se han definido.

```
PE1#show bgp vpnv4 unicast all summary
BGP router identifier 2.2.2.2, local AS number 1
BGP table version is 7, main routing table version 7
4 network entries using 624 bytes of memory
4 path entries using 320 bytes of memory
4/4 BGP path/bestpath attribute entries using 576 bytes of memory
2 BGP extended community entries using 80 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1600 total bytes of memory
BGP activity 4/0 prefixes, 4/0 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
3.3.3.3         4            1      13      14        7    0    0 00:08:20        2
```

f- *Configurar OSPF en los enlaces PE-CE*

Al configurar OSPF en los enlaces PE-CE, las rutas cliente deberán aparecer en las VRF de los nodos frontera:

```
PE1#show ip route vrf userA

Routing Table: userA
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      5.0.0.0/24 is subnetted, 1 subnets
O        5.5.5.0 [110/2] via 10.0.2.2, 00:06:35, FastEthernet1/0
      6.0.0.0/24 is subnetted, 1 subnets
B        6.6.6.0 [200/2] via 3.3.3.3, 00:04:48
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C        10.0.2.0/30 is directly connected, FastEthernet1/0
L        10.0.2.1/32 is directly connected, FastEthernet1/0
B        10.0.3.0/30 [200/0] via 3.3.3.3, 00:04:48
```

Se puede observar como existe una sesión OSPF con el equipo cliente directamente conectado (CE1) y una ruta BGP hacia CE2 y el enlace PE2-CE2.

Los valores entre corchetes indican la distancia administrativa, 110 para OSPF y 200 para BGP, y la métrica.

g- *Redistribución entre red cliente y red central*

La redistribución de ambas redes está constituida, por tanto, las tablas BGP ya disponen de las rutas de los equipos cliente para sus respectivas VRF.

```
PE1#show ip bgp vpnv4 vrf userA
BGP table version is 7, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf userA)
 *>  5.5.5.0/24       10.0.2.2                 2         32768 ?
 *>i 6.6.6.0/24       3.3.3.3                  2    100      0 ?
 *>  10.0.2.0/30      0.0.0.0                  0         32768 ?
 *>i 10.0.3.0/30      3.3.3.3                  0    100      0 ?
```

Con este comando, observando el apartado *Metric*, se verifica que, gracias a un protocolo IGP, PE1 tiene como vecino a PE2-CE2 y a CE2 a dos saltos.

Además, este elemento nos ofrece mayor claridad sobre el ***algoritmo BGP para escoger la mejor ruta***. Por orden de preferencia:

- Escoger el camino con el mayor "***Weight***"
- Escoger el camino con el mayor "***LocPrf***"
- Escoger el camino originado localmente
- Escoger el camino con el menor "***Path***"
- Escoger eBGP antes que iBGP
- Escoger el camino con la menor "***Metric***" hacia el siguiente salto BGP
- Cuando ambos caminos son externos escoger el más antiguo

En esta topología no se hace uso del algoritmo ya que solo existe una sesión BGP entre PE1 y PE2.

h- Comprobaciones finales

Al haber completado la configuración de la topología, debe existir solo conexión entre los equipos cliente con igual VRF. Con `traceroute` se mostrará el camino que realiza el tráfico vía la red central MPLS. Asimismo, la tabla de reenvío de todos los equipos estará completa.

```
PE1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      1.0.0.0/32 is subnetted, 3 subnets
O        1.0.1.1 [110/3] via 10.0.1.1, 00:10:50, FastEthernet0/0
O        1.1.1.1 [110/2] via 10.0.1.1, 00:10:50, FastEthernet0/0
O        1.2.1.1 [110/3] via 10.0.1.1, 00:10:50, FastEthernet0/0
      2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        2.2.2.0/24 is directly connected, Loopback0
L        2.2.2.2/32 is directly connected, Loopback0
      3.0.0.0/24 is subnetted, 1 subnets
O        3.3.3.0 [110/4] via 10.0.1.1, 00:09:34, FastEthernet0/0
      10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
O        10.0.0.0/30 [110/2] via 10.0.1.1, 00:10:50, FastEthernet0/0
O        10.0.0.4/30 [110/3] via 10.0.1.1, 00:10:50, FastEthernet0/0
C        10.0.1.0/30 is directly connected, FastEthernet0/0
L        10.0.1.2/32 is directly connected, FastEthernet0/0
O        10.0.1.4/30 [110/3] via 10.0.1.1, 00:10:50, FastEthernet0/0
O        10.0.1.8/30 [110/2] via 10.0.1.1, 00:10:50, FastEthernet0/0
```

- *Ejemplo de CE1 y CE2*

```
CE1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     5.0.0.0/24 is subnetted, 1 subnets
C       5.5.5.0 is directly connected, Loopback0
     6.0.0.0/24 is subnetted, 1 subnets
O E2    6.6.6.0 [110/1] via 10.0.2.1, 00:06:06, FastEthernet0/0
     10.0.0.0/30 is subnetted, 2 subnets
C       10.0.2.0 is directly connected, FastEthernet0/0
O E2    10.0.3.0 [110/1] via 10.0.2.1, 00:06:06, FastEthernet0/0
```

Las rutas OSPF aparecen como tipo 2, tipo por defecto en el cual la métrica de una ruta es siempre la externa independientemente de la métrica interna para alcanzar dicha ruta.

```
CE1#traceroute 6.6.6.6

Type escape sequence to abort.
Tracing the route to 6.6.6.6

  1 10.0.2.1 48 msec 92 msec 92 msec
  2 10.0.1.1 [MPLS: Labels 21/24 Exp 0] 624 msec 524 msec 752 msec
  3 10.0.1.10 [MPLS: Labels 21/24 Exp 0] 784 msec 656 msec 856 msec
  4 10.0.3.1 [MPLS: Label 24 Exp 0] 580 msec 560 msec 492 msec
  5 10.0.3.2 704 msec 680 msec 684 msec
```

```
CE2#traceroute 5.5.5.5

Type escape sequence to abort.
Tracing the route to 5.5.5.5

  1 10.0.3.1 140 msec 136 msec 100 msec
  2 10.0.1.5 [MPLS: Labels 20/24 Exp 0] 468 msec 392 msec 476 msec
  3 10.0.1.9 [MPLS: Labels 20/24 Exp 0] 408 msec 492 msec 488 msec
  4 10.0.2.1 [MPLS: Label 24 Exp 0] 620 msec 500 msec 556 msec
  5 10.0.2.2 628 msec 752 msec 612 msec
```

4. Enunciado de la práctica

Este proyecto se basa principalmente en el desarrollo de una topología MPLS VPN usada posteriormente como enunciado de una práctica de asignaturas de grado o máster.

En toda práctica los ejercicios deben ser claros y precisos. Estos deben plantearse de manera que el alumno pueda obtener un mayor aprendizaje sobre las tecnologías previamente estudiadas.

Asimismo, la suma de las cuestiones debe estar sujeta a un tiempo determinado, el cual será establecido por el profesor correspondiente. En este caso, la práctica indicada tendrá una duración de unas dos horas.

El enunciado lo componen ocho preguntas, cuatro relacionadas con la topología definida en el apartado *3.5* y otras cuatro, con otra topología más compleja.

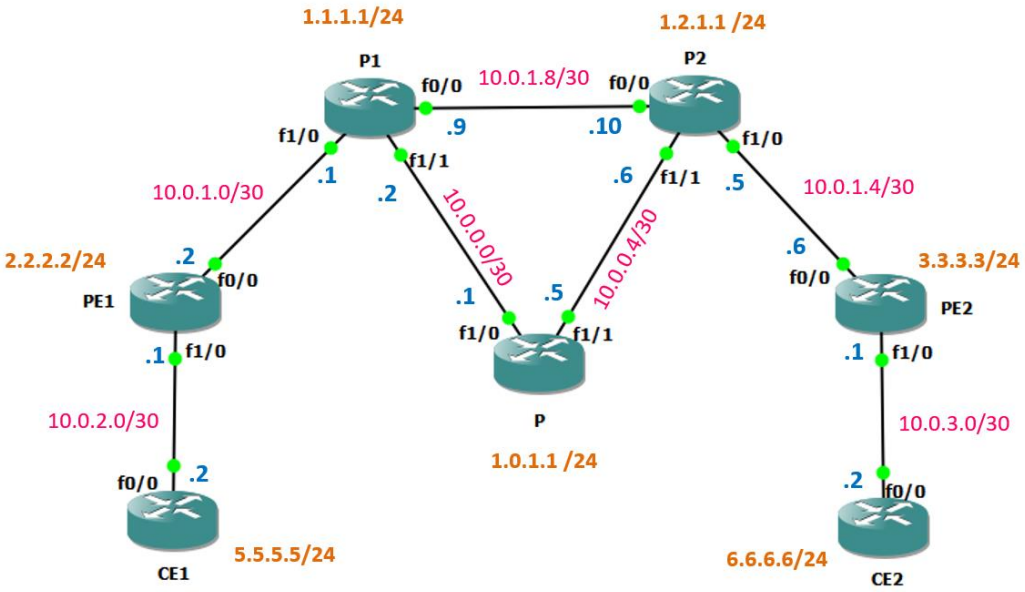
Se definen dos topologías diferentes con el objetivo de estudiar en mayor profundidad las características de estas redes MPLS VPN. La primera, y más básica, se centra más en el *backbone*, y la segunda o modificación, en las redes cliente.

A continuación, se presenta el enunciado de la práctica:

PRÁCTICA: VPN DE NIVEL 3 SOBRE UNA RED MPLS

En este laboratorio se va a estudiar el funcionamiento a nivel práctico del conjunto de las redes MPLS VPN.

1. Contamos con la siguiente topología donde los equipos P, P1 y P2 constituyen el proveedor de servicios (SP) o red central y CE1, CE2 pertenecen a la red cliente.



a- Indica cuáles son los protocolos usados en cada enlace

b- Una vez que sabemos el protocolo usado en la red central, podemos observar concretamente las interfaces de los equipos que la forman. Ejecuta el comando `show mpls interfaces` **¿qué nueva información nos aportan?, ¿qué implica la activación de este nuevo protocolo?**

c- Gracias a la herramienta Wireshark, captura los paquetes enviados por el enlace PE1-P1. Analiza estos paquetes al hacer un ping de CE1 a CE2**, ¿qué diferencias observas respecto a una red MPLS habitual?**

d- Esta vez fíjate en los paquetes LDP de la captura, **¿qué información nos muestran?**

2. A continuación, dejamos atrás esta topología para dar paso a una nueva, que nos permitirá aclarar en mayor profundidad el funcionamiento de las redes VPN y sus conceptos.

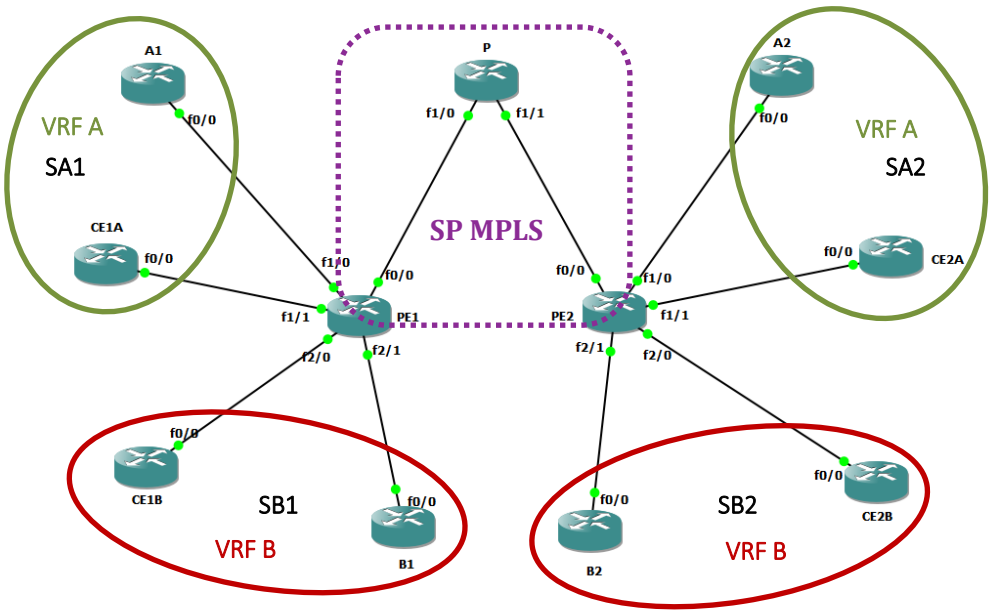


Figura 20. Distribución topología 2

En esta segunda topología, como se puede contemplar, el SP se ha reducido a un *router* P y dos *routers* frontera. Sin embargo, las nuevas redes cliente cuentan con seis nuevos equipos distribuidos en cuatro sedes pertenecientes a dos VRFs diferenciadas.

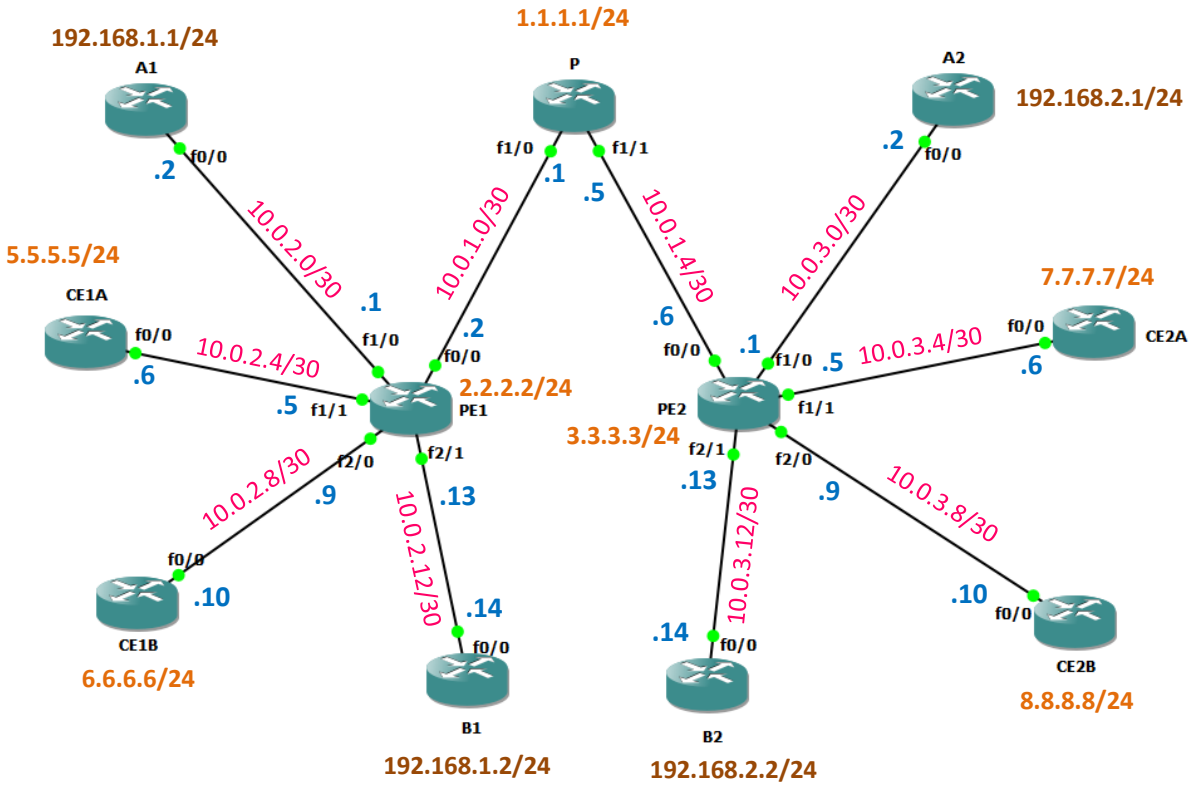


Figura 21. Rutas topología 2

a- Ejecuta el comando `show ip bgp vpnv4 vrf userA` en PE1, **¿cuáles son sus nodos vecinos BGP? ¿Qué implica el valor *local preference*?**

b- **Completa la configuración de esta topología con el desarrollo de CE1B, B1, CE2B** y **B2** teniendo en cuenta que los equipos cliente solo pueden establecer conexión entre aquellos que contengan en su nombre la misma letra. (Sede A1 <-> Sede A2, Sede B1 <-> Sede B2)

c- Realiza las comprobaciones necesarias para verificar el correcto funcionamiento de las configuraciones anteriores. Los comandos utilizados deben aportar certeza sobre la totalidad de los procesos que definen la topología.

d- Explica los conceptos RD y VRF. Muestra los correspondientes de esta topología.

5. Solución de la práctica

Una vez definido el enunciado de la práctica, se muestran seguidamente las posibles soluciones para cada una de las cuestiones.

1. *Todas aquellas respuestas que hagan uso de ciertos comandos estarán acompañadas por las capturas correspondientes, a no ser que ya se hayan mostrado en el apartado **3.5.2** como análisis de pruebas.*

a- Para conocer los protocolos usados en esta topología podemos hacer uso de varios comandos:

- La primera opción sería simplemente acceder a la configuración completa de la topología y así observar cómo está definido cada uno de los procesos e interfaces -para ello se usa **`show run.`** La información necesaria se obtiene igualmente con **`show ip protocols`**. (Distance = 110 -- OSPF, Distance = 200 -- iBGP)

```
PE1#show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 2.2.2.2
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    2.2.2.0 0.0.0.255 area 0
    10.0.1.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    3.3.3.3              110      00:11:58
    1.1.1.1              110      00:13:13
    1.0.1.1              110      00:13:13
    1.2.1.1              110      00:13:13
  Distance: (default is 110)

Routing Protocol is "bgp 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  IGP synchronization is disabled
  Automatic route summarization is disabled
  Neighbor(s):
    Address          FiltIn FiltOut DistIn DistOut Weight RouteMap
    3.3.3.3
  Maximum path: 1
  Routing Information Sources:
    Gateway         Distance      Last Update
    3.3.3.3              200      00:07:58
  Distance: external 20 internal 200 local 200
```

- Otra manera sería ejecutando **`show ip route`** en cualquiera de los nodos. De esta forma, gracias a las tablas de rutas se observan los protocolos usados en el reenvío de los paquetes.
  En este caso, conocer el uso de BGP no es posible.

- De igual modo, si se hace uso de **`traceroute`**, se contemplará que en la red central el protocolo definido es MPLS.

- Por último, podemos hacer uso de la aplicación *Wireshark*, que mediante distintos filtros nos indicará los paquetes enviados por cada enlace.

b- Cuando empleamos **`show mpls interfaces`** se observa la activación del protocolo LDP. Según las respuestas obtenidas en la cuestión **a-**, este protocolo no ha sido configurado literalmente. LDP se acciona en las interfaces configuradas como MPLS para la distribución de las etiquetas MPLS entre los distintos nodos de la red central.

- *Ejemplo de P1*

```
P1#show mpls interfaces
Interface              IP           Tunnel   BGP Static Operational
FastEthernet0/0        Yes (ldp)    No       No  No     Yes
FastEthernet1/0        Yes (ldp)    No       No  No     Yes
FastEthernet1/1        Yes (ldp)    No       No  No     Yes
```

Si se quiere conocer más acerca del uso de LDP en la topología, se puede ejecutar:

- **`show mpls ldp bindings`** para conocer cuál ha sido la etiqueta a usar para enviar el tráfico (LIB),

- **`show mpls ldp discovery`** para cerciorarse de que el protocolo está activo y mandando mensajes saludo, o

- **`show mpls ldp neighbor`**, que muestra los saltos usados para llegar a otros nodos LDP y más información de interés.

```
P1#show mpls ldp binding
  lib entry: 1.0.1.0/24, rev 13
        remote binding: lsr: 1.0.1.1:0, label: imp-null
  lib entry: 1.0.1.1/32, rev 10
        local binding:  label: 16
        remote binding: lsr: 1.2.1.1:0, label: 16
        remote binding: lsr: 2.2.2.2:0, label: 16
  lib entry: 1.1.1.0/24, rev 2
        local binding:  label: imp-null
  lib entry: 1.1.1.1/32, rev 14
        remote binding: lsr: 1.0.1.1:0, label: 16
        remote binding: lsr: 1.2.1.1:0, label: 17
        remote binding: lsr: 2.2.2.2:0, label: 17
  lib entry: 1.2.1.0/24, rev 19
        remote binding: lsr: 1.2.1.1:0, label: imp-null
  lib entry: 1.2.1.1/32, rev 16
```

```
P1#show mpls ldp discovery
 Local LDP Identifier:
    1.1.1.1:0
    Discovery Sources:
    Interfaces:
        FastEthernet0/0 (ldp): xmit/recv
            LDP Id: 1.2.1.1:0
        FastEthernet1/0 (ldp): xmit/recv
            LDP Id: 2.2.2.2:0
        FastEthernet1/1 (ldp): xmit/recv
            LDP Id: 1.0.1.1:0
```

```
P1#show mpls ldp neighbor
    Peer LDP Ident: 1.0.1.1:0; Local LDP Ident 1.1.1.1:0
        TCP connection: 1.0.1.1.646 - 1.1.1.1.62197
        State: Oper; Msgs sent/rcvd: 17/17; Downstream
        Up time: 00:04:35
        LDP discovery sources:
          FastEthernet1/1, Src IP addr: 10.0.0.1
        Addresses bound to peer LDP Ident:
          10.0.0.1        10.0.0.5        1.0.1.1
    Peer LDP Ident: 2.2.2.2:0; Local LDP Ident 1.1.1.1:0
        TCP connection: 2.2.2.2.34921 - 1.1.1.1.646
        State: Oper; Msgs sent/rcvd: 16/16; Downstream
        Up time: 00:03:38
        LDP discovery sources:
          FastEthernet1/0, Src IP addr: 10.0.1.2
        Addresses bound to peer LDP Ident:
          10.0.1.2        2.2.2.2
    Peer LDP Ident: 1.2.1.1:0; Local LDP Ident 1.1.1.1:0
        TCP connection: 1.2.1.1.53515 - 1.1.1.1.646
        State: Oper; Msgs sent/rcvd: 15/15; Downstream
        Up time: 00:03:07
        LDP discovery sources:
          FastEthernet0/0, Src IP addr: 10.0.1.10
        Addresses bound to peer LDP Ident:
          10.0.1.10       10.0.1.5        10.0.0.6        1.2.1.1
```

c-

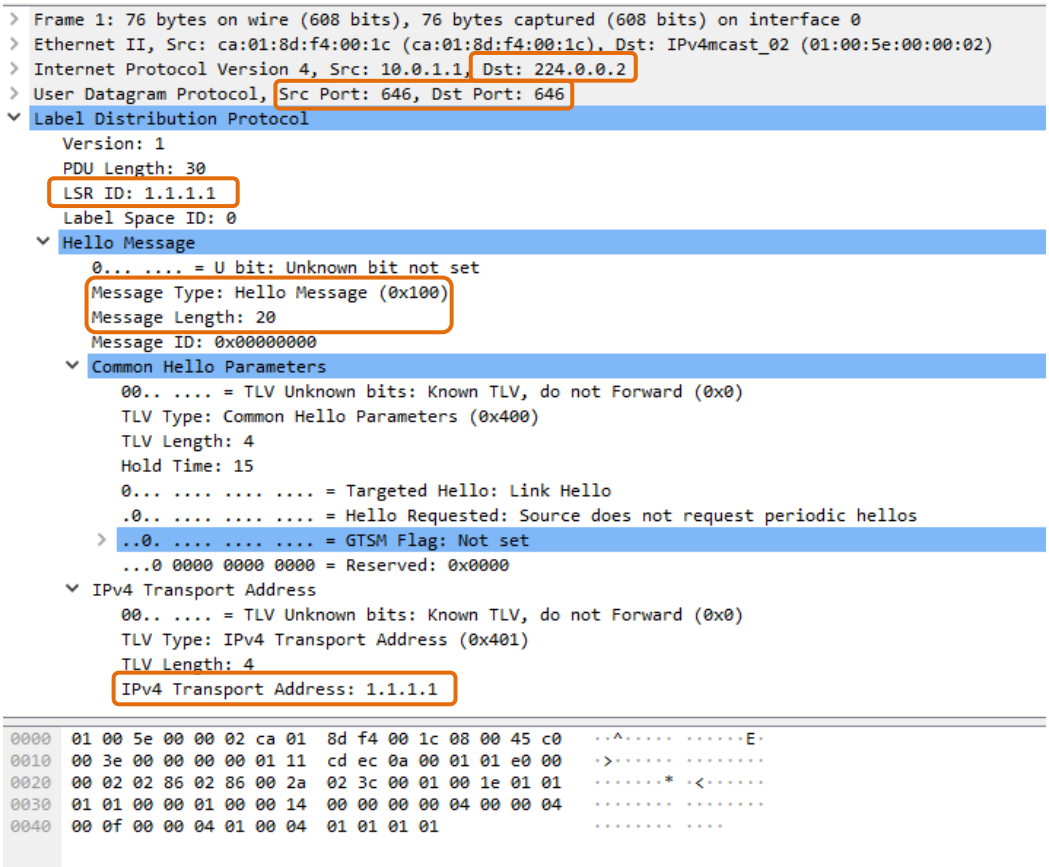
```
> Frame 24: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface 0
v Ethernet II, Src: ca:05:1d:e8:00:00 (ca:05:1d:e8:00:00), Dst: ca:01:8d:f4:00:1c (ca:01:8d:f4:00:1c)
  > Destination: ca:01:8d:f4:00:1c (ca:01:8d:f4:00:1c)
  > Source: ca:05:1d:e8:00:00 (ca:05:1d:e8:00:00)
    Type: MPLS label switched packet (0x8847)
v MultiProtocol Label Switching Header, Label: 21, Exp: 0, S: 0, TTL: 254
    0000 0000 0000 0001 0101 .... .... .... = MPLS Label: 21
    .... .... .... .... .... 000. .... .... = MPLS Experimental Bits: 0
    .... .... .... .... .... ...0 .... .... = MPLS Bottom Of Label Stack: 0
    .... .... .... .... .... .... 1111 1110 = MPLS TTL: 254
v MultiProtocol Label Switching Header, Label: 24, Exp: 0, S: 1, TTL: 254
    0000 0000 0000 0001 1000 .... .... .... = MPLS Label: 24
    .... .... .... .... .... 000. .... .... = MPLS Experimental Bits: 0
    .... .... .... .... .... ...1 .... .... = MPLS Bottom Of Label Stack: 1
    .... .... .... .... .... .... 1111 1110 = MPLS TTL: 254
> Internet Protocol Version 4, Src: 10.0.2.2, Dst: 6.6.6.6
> Internet Control Message Protocol
```

```
0000  ca 01 8d f4 00 1c ca 05  1d e8 00 00 88 47 00 01   ........ .....G..
0010  50 fe 00 01 81 fe 45 00  00 64 00 14 00 00 fe 01   P.....E. .d......
0020  a4 77 0a 00 02 02 06 06  06 06 08 00 62 ba 00 04   .w...... ....b...
0030  00 00 00 00 00 00 00 18  1b 74 ab cd ab cd ab cd   ........ .t......
0040  ab cd ab cd ab cd ab cd  ab cd ab cd ab cd ab cd   ........ ........
0050  ab cd ab cd ab cd ab cd  ab cd ab cd ab cd ab cd   ........ ........
0060  ab cd ab cd ab cd ab cd  ab cd ab cd ab cd ab cd   ........ ........
0070  ab cd ab cd ab cd ab cd  ab cd                     ........ ..
```

Como se puede ver, estos paquetes constan de dos etiquetas MPLS, en vez de una, una para la ruta VPN y otra para la ruta OSPF.

La cabecera MPLS de estos paquetes nos permite, asimismo, identificar cuál es la etiqueta asociada a cada proceso. El bit S a 0 indica que es la primera etiqueta y por tanto la usada en la ruta VPN (en este caso *label*: 21). Por lo tanto, la restante será aquella que identifica el proceso OSPF (en este caso *label*: 24).

d-



- Estos mensajes "*Hello*" LDP se envían a la dirección *multicast* 224.0.0.2 con puerto UDP origen y destino 646.
- Cada *router* tiene un identificador único, LSR ID, el cual está normalmente relacionado con la dirección de *loopback* del nodo.
- La dirección IPV4 de transporte es la usada en la conexión TCP y, al igual que el LSR ID, es igual a la dirección *loopback*.
- Además, se pueden distinguir otros campos de interés como el tamaño o el tipo de mensaje.

2.

a-

```
PE1#show ip bgp vpnv4 vrf userA
BGP table version is 45, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf userA)
 *>  5.5.5.0/24       10.0.2.6                 2         32768 ?
 *>i 7.7.7.0/24       3.3.3.3                  2    100      0 ?
 *>  10.0.2.0/30      0.0.0.0                  0         32768 ?
 *>  10.0.2.4/30      0.0.0.0                  0         32768 ?
 *>i 10.0.3.0/30      3.3.3.3                  0    100      0 ?
 *>i 10.0.3.4/30      3.3.3.3                  0    100      0 ?
 *>  192.168.1.0      10.0.2.2                 2         32768 ?
 *>  192.168.1.1/32   0.0.0.0                  0         32768 ?
 *>  192.168.1.2/32   0.0.0.0                  0         32768 ?
 *>i 192.168.2.0      3.3.3.3                  2    100      0 ?
```

Este comando muestra la existencia de una conexión directa con todos aquellos enlaces en los que su apartado ***Metric*** sea igual a 0. Para la VRF `userA` en PE1, se tienen como vecinos los enlaces PE1-A1, PE1-CE1A, PE2-A2 y PE2-CE2A -estos últimos gracias a un protocolo IGP.

Asimismo, se puede observar que existe conexión entre los equipos de diferentes sedes que pertenecen a la misma VRF.

- *Local Preference* es un atributo que permite determinar, a ciertos equipos, la mejor ruta hacia el destino. Si un router tiene varias sesiones BGP activas y recibe una ruta por cada sesión hacia un destino, se escogerá aquella ruta con mayor ***LocPref***.

  En este caso, 100 es el valor por defecto y equivale a no disponer de ***LocPref***, por lo que todas las rutas tienen la misma preferencia.

  En esta topología no se hace uso de este atributo ya que solo existe una sesión BGP, aun así, es importante conocer su significado.

b- La manera más sencilla sería observar, primeramente, la configuración dada, para más tarde completar la nueva requerida con los mismos métodos. Para ello, se ejecuta **`show run`** en todos los equipos:

PE1	PE2

ip vrf userA
  rd 1:1
  route-target both 1:1
 	
interface Loopback0
  ip address 2.2.2.2 255.255.255.0
  ip ospf network point-to-point
!
interface Loopback111
 description lo int for userA vrf
 ip ospf network point-to-point
 ip vrf forwarding userA
 ip address 192.168.1.1 255.255.255.255
!
interface Loopback112
 description lo int for userA vrf
 ip ospf network point-to-point
 ip vrf forwarding userA
 ip address 192.168.1.2 255.255.255.255
!
interface FastEthernet0/0
  ip address 10.0.1.2 255.255.255.252
  duplex full
  mpls ip
!
interface FastEthernet1/0
  description connection to the userA router
  ip vrf forwarding userA
  ip address 10.0.2.1 255.255.255.252
  ip ospf 2 area 0
  speed auto
  duplex auto
!
interface FastEthernet1/1
  description connection to the userA router
  ip vrf forwarding userA
  ip address 10.0.2.5 255.255.255.252
  ip ospf 2 area 0
  speed auto
  duplex auto
!
router ospf 2 vrf userA
  router-id 10.0.2.1
  net 192.168.1.0 0.0.0.3 area 0
  capability vrf-lite
  redistribute bgp 1 subnets
!
router ospf 1
  router-id 2.2.2.2
  network 2.2.2.0 0.0.0.255 area 0
  network 10.0.1.0 0.0.0.3 area 0
!
router bgp 1
  bgp log-neighbor-changes
  neighbor 3.3.3.3 remote-as 1
  neighbor 3.3.3.3 update-source Loopback0
 !
  address-family vpnv4
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community extended
  exit-address-family
  !
	ip vrf userA
	  rd 1:1
	  route-target both 1:1
	
	interface Loopback0
	  ip address 3.3.3.3 255.255.255.0
	  ip ospf network point-to-point
	!
	interface Loopback121
	 description lo int for userA vrf
	 ip ospf network point-to-point
	 ip vrf forwarding userA
	 ip address 192.168.2.1 255.255.255.255
	!
	interface Loopback122
	 description lo int for userA vrf
	 ip ospf network point-to-point
	 ip vrf forwarding userA
	 ip address 192.168.2.2 255.255.255.255
	!
	interface FastEthernet0/0
	  ip address 10.0.1.6 255.255.255.252
	  duplex full
	  mpls ip
	!
	interface FastEthernet1/0
	  description connection to the userA router
	  ip vrf forwarding userA
	  ip address 10.0.3.1 255.255.255.252
	  ip ospf 2 area 0
	  speed auto
	  duplex auto
	!
	interface FastEthernet1/1
	  description connection to the userA router
	  ip vrf forwarding userA
	  ip address 10.0.3.5 255.255.255.252
	  ip ospf 2 area 0
	  speed auto
	  duplex auto
	!
	router ospf 2 vrf userA
	  router-id 10.0.3.1
	  net 192.168.2.0 0.0.0.0 area 0
	  capability vrf-lite
	  redistribute bgp 1 subnets
	!
	router ospf 1
	  router-id 3.3.3.3
	  network 3.3.3.0 0.0.0.255 area 0
	  network 10.0.1.4 0.0.0.3 area 0
	!
	router bgp 1
	  bgp log-neighbor-changes
	  neighbor 2.2.2.2 remote-as 1
	  neighbor 2.2.2.2 update-source Loopback0
	  !
	  address-family vpnv4
	  neighbor 2.2.2.2 activate
	  neighbor 2.2.2.2 send-community extended
	  exit-address-family
	  !

```
   address-family ipv4 vrf userA
   redistribute ospf 2
   exit-address-family
   !
   address-family ipv4 vrf userB
   exit-address-family
   !
```

```
  address-family ipv4 vrf userA
    redistribute ospf 2
    exit-address-family
  !
  address-family ipv4 vrf userB
  exit-address-family
  !
```

P

```
interface Loopback0
  ip address 1.1.1.1 255.255.255.0
!
interface FastEthernet0/0
  no ip address
  shutdown
  duplex full
!
interface FastEthernet1/0
  ip address 10.0.1.1 255.255.255.252
  speed auto
  duplex auto
  mpls ip
!
interface FastEthernet1/1
  ip address 10.0.1.5 255.255.255.252
  speed auto
  duplex auto
  mpls ip
!
router ospf 1
  router-id 1.1.1.1
  network 1.1.1.0 0.0.0.255 area 0
  network 10.0.1.0 0.0.0.3 area 0
  network 10.0.1.4 0.0.0.3 area 0
!
```

A1

```
interface Loopback0
  ip address 192.168.1.1 255.255.255.0
  ip ospf network point-to-point
  ip ospf 1 area 0
!
interface FastEthernet0/0
  ip address 10.0.2.2 255.255.255.252
  ip ospf 1 area 0
  duplex auto
  speed auto
!
router ospf 1
  router-id 192.168.1.1
  log-adjacency-changes
  network 192.168.1.0 0.0.0.3 area 0
```

CE1A

```
interface Loopback0
 ip address 5.5.5.5 255.255.255.0
 ip ospf network point-to-point
 ip ospf 1 area 0
!
interface FastEthernet0/0
 ip address 10.0.2.6 255.255.255.252
 ip ospf 1 area 0
 duplex auto
 speed auto
!
router ospf 1
 router-id 5.5.5.5
 network 192.168.1.0 0.0.0.3 area 0
 log-adjacency-changes
```

A2

```
interface Loopback0
 ip address 192.168.2.1 255.255.255.0
 ip ospf network point-to-point
 ip ospf 1 area 0
!
interface FastEthernet0/0
 ip address 10.0.3.2 255.255.255.252
 ip ospf 1 area 0
 duplex auto
 speed auto
 !
router ospf 1
 router-id 192.168.2.1
 log-adjacency-changes
 network 192.168.2.0 0.0.0.3 area 0
```

CE2A

```
interface Loopback0
 ip address 7.7.7.7255.255.255.0
 ip ospf network point-to-point
 ip ospf 1 area 0
!
interface FastEthernet0/0
 ip address 10.0.3.6 255.255.255.252
 ip ospf 1 area 0
 duplex auto
 speed auto
 !
router ospf 1
 router-id 7.7.7.7
 log-adjacency-changes
 network 192.168.2.0 0.0.0.3 area 0
```

Tabla 5. Configuración predefinida topología 2

Las configuraciones anteriores son bastante parecidas a aquellas de la topología básica *[3.4.1]*. Sin embargo, al configurar las nuevas sedes se comenzarán a observar los primeros cambios.

- Configuración final con las modificaciones destacadas en color morado (*no se muestran los nodos P, A1, A2, CE1A y CE2A ya que no experimentan cambios*):

PE1	PE2

ip vrf userA
  rd 1:1
  route-target both 1:1
ip vrf userB
  rd 2:2
  route-target both 2:2
 	
interface Loopback0
  ip address 2.2.2.2 255.255.255.0
  ip ospf network point-to-point
!
interface Loopback111
  description lo int for userA vrf
  ip ospf network point-to-point
  ip vrf forwarding userA
  ip address 192.168.1.1 255.255.255.255
!
interface Loopback112
  description lo int for userA vrf
  ip ospf network point-to-point
  ip vrf forwarding userA
  ip address 192.168.1.2 255.255.255.255
!
interface Loopback211
  description lo int for userB vrf
  ip ospf network point-to-point
  ip vrf forwarding userB
  ip address 192.168.1.1 255.255.255.255
!
interface Loopback212
  description lo int for userB vrf
  ip ospf network point-to-point
  ip vrf forwarding userB
  ip address 192.168.1.2 255.255.255.255
!
 	
interface FastEthernet0/0
  ip address 10.0.1.2 255.255.255.252
  duplex full
  mpls ip
!
interface FastEthernet1/0
  description connection to the userA router
  ip vrf forwarding userA
  ip address 10.0.2.1 255.255.255.252
  ip ospf 2 area 0
  speed auto
  duplex auto
	ip vrf userA
	  rd 1:1
	  route-target both 1:1
	ip vrf userB
	  rd 2:2
	  route-target both 2:2
	
	interface Loopback0
	  ip address 3.3.3.3 255.255.255.0
	  ip ospf network point-to-point
	!
	interface Loopback121
	  description lo int for userA vrf
	  ip ospf network point-to-point
	  ip vrf forwarding userA
	  ip address 192.168.2.1 255.255.255.255
	!
	interface Loopback122
	  description lo int for userA vrf
	  ip ospf network point-to-point
	  ip vrf forwarding userA
	  ip address 192.168.2.2 255.255.255.255
	!
	interface Loopback221
	  description lo int for userB vrf
	  ip ospf network point-to-point
	  ip vrf forwarding userB
	  ip address 192.168.2.1 255.255.255.255
	!
	interface Loopback222
	  description lo int for userB vrf
	  ip ospf network point-to-point
	  ip vrf forwarding userB
	  ip address 192.168.2.2 255.255.255.255
	!
	
	interface FastEthernet0/0
	  ip address 10.0.1.6 255.255.255.252
	  duplex full
	  mpls ip
	!
	interface FastEthernet1/0
	  description connection to the userA router
	  ip vrf forwarding userA
	  ip address 10.0.3.1 255.255.255.252
	  ip ospf 2 area 0
	  speed auto
	  duplex auto

```
!
interface FastEthernet1/1
  description connection to the userA router
  ip vrf forwarding userA
  ip address 10.0.2.5 255.255.255.252
  ip ospf 2 area 0
  speed auto
  duplex auto
!
interface FastEthernet2/0
  description connection to the userB router
  ip vrf forwarding userB
  ip address 10.0.2.9 255.255.255.252
  ip ospf 3 area 0
  speed auto
  duplex auto
!
interface FastEthernet2/1
  description connection to the userB router
  ip vrf forwarding userB
  ip address 10.0.2.13 255.255.255.252
  ip ospf 3 area 0
  speed auto
  duplex auto
!
router ospf 2 vrf userA
  router-id 10.0.2.1
  net 192.168.1.0 0.0.0.3 area 0
  capability vrf-lite
  redistribute bgp 1 subnets
!
router ospf 3 vrf userB
  router-id 10.0.2.9
  net 192.168.1.0 0.0.0.3 area 0
  capability vrf-lite
  redistribute bgp 1 subnets
!


router ospf 1
  router-id 2.2.2.2
  network 2.2.2.0 0.0.0.255 area 0
  network 10.0.0.1 0.0.0.3 area 0
!
router bgp 1
  bgp log-neighbor-changes
  neighbor 3.3.3.3 remote-as 1
  neighbor 3.3.3.3 update-source Loopback0
 !
  address-family vpnv4
    neighbor 3.3.3.3 activate
    neighbor 3.3.3.3 send-community extended
    exit-address-family
   !
   address-family ipv4 vrf userA
     redistribute ospf 2
     exit-address-family
   !
   address-family ipv4 vrf userB
     redistribute ospf 3
     exit-address-family
   !
```

```
!
interface FastEthernet1/1
  description connection to the userA router
  ip vrf forwarding userA
  ip address 10.0.3.5 255.255.255.252
  ip ospf 2 area 0
  speed auto
  duplex auto
!
interface FastEthernet2/0
  description connection to the userB router
  ip vrf forwarding userB
  ip address 10.0.3.9 255.255.255.252
  ip ospf 3 area 0
  speed auto
  duplex auto
!
interface FastEthernet2/1
  description connection to the userB router
  ip vrf forwarding userB
  ip address 10.0.3.13 255.255.255.252
  ip ospf 3 area 0
  speed auto
  duplex auto
!
router ospf 2 vrf userA
  router-id 10.0.3.1
  net 192.168.2.0 0.0.0.0 area 0
  capability vrf-lite
  redistribute bgp 1 subnets
!
router ospf 3 vrf userB
  router-id 10.0.3.9
  net 192.168.2.0 0.0.0.0 area 0
  capability vrf-lite
  redistribute bgp 1 subnets
!


router ospf 1
  router-id 3.3.3.3
  network 3.3.3.0 0.0.0.255 area 0
  network 10.0.1.4 0.0.0.3 area 0
!
router bgp 1
  bgp log-neighbor-changes
  neighbor 2.2.2.2 remote-as 1
  neighbor 2.2.2.2 update-source Loopback0
  !
  address-family vpnv4
    neighbor 2.2.2.2 activate
    neighbor 2.2.2.2 send-community extended
    exit-address-family
  !
  address-family ipv4 vrf userA
    redistribute ospf 2
    exit-address-family
  !
  address-family ipv4 vrf userB
    redistribute ospf 3
    exit-address-family
  !
```

CE1B	B1

interface Loopback0
  ip address 6.6.6.6 255.255.255.0
  ip ospf network point-to-point
  ip ospf 1 area 0
!
interface FastEthernet0/0
  ip address 10.0.2.10 255.255.255.252
  ip ospf 1 area 0
  duplex auto
  speed auto
!
router ospf 1
 router-id 6.6.6.6
 log-adjacency-changes
 network 192.168.1.0 0.0.0.3 area 0
	interface Loopback0
	  ip address 192.168.1.2 255.255.255.0
	  ip ospf network point-to-point
	  ip ospf 1 area 0
	!
	interface FastEthernet0/0
	  ip address 10.0.2.14 255.255.255.252
	  ip ospf 1 area 0
	  duplex auto
	  speed auto
	!
	router ospf 1
	  router-id 192.168.1.2
	  log-adjacency-changes
	  network 192.168.1.0 0.0.0.3 area 0

CE2B	**B2**

interface Loopback0
  ip address 8.8.8.8 255.255.255.0
  ip ospf network point-to-point
  ip ospf 1 area 0
!
interface FastEthernet0/0
  ip address 10.0.3.10 255.255.255.252
  ip ospf 1 area 0
  duplex auto
  speed auto
!
router ospf 1
 router-id 8.8.8.8
 log-adjacency-changes
 network 192.168.2.0 0.0.0.3 area 0
	interface Loopback0
	  ip address 192.168.2.2 255.255.255.0
	  ip ospf network point-to-point
	  ip ospf 1 area 0
	!
	interface FastEthernet0/0
	  ip address 10.0.3.14 255.255.255.252
	  ip ospf 1 area 0
	  duplex auto
	  speed auto
	!
	router ospf 1
	 router-id 192.168.2.2
	 log-adjacency-changes
	 network 192.168.2.0 0.0.0.3 area 0

Tabla 6. Configuración completa topología 2

Asignar una interfaz loopback a una VRF es cuestión de seguridad. Una interfaz de este tipo, siempre que el equipo está activo, está disponible, por lo que les permite a las diferentes sesiones de protocolos asociadas estar activas incluso si la interfaz de salida correspondiente se ha caído.

c- El comando que verificará de manera más adecuada el correcto funcionamiento total de la red es `traceroute.` Desde los nodos cliente se pueden ver las conexiones existentes entre las diferentes VPNs.

Podemos hacer uso igualmente del comando `ping`, pero aporta menor claridad.

- *Entre VPNs con igual VRF:*

  - **A2-CE2A**

```
A2#traceroute 7.7.7.7

Type escape sequence to abort.
Tracing the route to 7.7.7.7

  1 10.0.3.1 352 msec 388 msec 208 msec
  2 10.0.3.6 564 msec 544 msec 624 msec
```

  - **A1-A2:**

```
A1#traceroute 192.168.2.1

Type escape sequence to abort.
Tracing the route to 192.168.2.1

  1 10.0.2.1 380 msec 216 msec 300 msec
  2 10.0.1.1 [MPLS: Labels 17/22 Exp 0] 1372 msec 1236 msec 1200 msec
  3 10.0.3.1 [MPLS: Label 22 Exp 0] 1040 msec 968 msec 616 msec
  4 10.0.3.2 1264 msec 1376 msec 1336 msec
```

  - **CE2B-B2:**

```
CE2B#traceroute 192.168.2.2

Type escape sequence to abort.
Tracing the route to 192.168.2.2

  1 10.0.3.9 320 msec 204 msec 296 msec
```

  - **CE1B-CE2B:**

```
CE1B#traceroute 8.8.8.8

Type escape sequence to abort.
Tracing the route to 8.8.8.8

  1 10.0.2.9 360 msec 272 msec 372 msec
  2 10.0.1.1 [MPLS: Labels 17/23 Exp 0] 1328 msec 1360 msec 1328 msec
  3 10.0.3.9 [MPLS: Label 23 Exp 0] 1048 msec 1032 msec 1156 msec
  4 10.0.3.10 1404 msec 1688 msec 1252 msec
```

- *Entre VPN con distinta VRF:*

  - **CE1B-CE1A y CE1B-CE2A:**

```
CE1B#ping 5.5.5.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.5.5.5, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
CE1B#
CE1B#ping 7.7.7.7

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 7.7.7.7, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Como se puede observar, solo existe comunicación entre redes con igual VRF.

d- *RD (Route Distinguisher)*: identificador numérico situado delante de la dirección IPv4, el cual la convierte en única dentro de un dominio MPLS.

VRF (Virtual Routing and Forwarding): Combinación de las tablas de direccionamiento y envío IP creadas para cada VPN en el PE.

Contaremos con dos VRF distintas, una para `userA` ya predefinida, y otra para `userB` que será aquella incluida por el alumno en la cuestión anterior.

```
PE1#show run | begin vrf
ip vrf userA
 rd 1:1
 route-target export 1:1
 route-target import 1:1
!
ip vrf userB
 rd 2:2
 route-target export 2:2
 route-target import 2:2
!
```

- A continuación, aunque el enunciado de la práctica no lo indique, se ofrecen capturas añadidas de esta segunda topología como prueba de su correcto funcionamiento:

  - *Comprobación de interfaces asignadas a cada VRF:*

```
PE1#show ip vrf interfaces
Interface              IP-Address      VRF                              Protocol
Lo111                  192.168.1.1     userA                            up
Lo112                  192.168.1.2     userA                            up
Fa1/0                  10.0.2.1        userA                            up
Fa1/1                  10.0.2.5        userA                            up
Lo211                  192.168.1.1     userB                            up
Lo212                  192.168.1.2     userB                            up
Fa2/0                  10.0.2.9        userB                            up
Fa2/1                  10.0.2.13       userB                            up
```

  - *Comunicación entre diferentes clientes pertenecientes a igual o distinta VRF:*

    No se obtienen datos desde la VRF `userA` a direcciones asociadas a la VRF `userB` y viceversa.

```
PE1#ping vrf userA 10.0.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 200/316/512 ms
PE1#
PE1#ping vrf userB 10.0.2.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.2.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 88/281/524 ms
PE1#
PE1#ping vrf userA 10.0.2.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.2.10, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
PE1#
PE1#ping vrf userB 10.0.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.2.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
PE1#
```

- *Tablas de rutas de dos de los clientes, uno de cada sede, donde se ve claramente lo dicho anteriormente, las direcciones de cada VRF están aisladas de aquellas que no pertenecen a la misma. En estas tablas se pueden observar también los protocolos usados en cada enlace, así como el número de saltos a realizar para llegar a destino.*

```
A1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     5.0.0.0/24 is subnetted, 1 subnets
O       5.5.5.0 [110/3] via 10.0.2.1, 00:29:13, FastEthernet0/0
     7.0.0.0/24 is subnetted, 1 subnets
O E2    7.7.7.0 [110/1] via 10.0.2.1, 00:22:16, FastEthernet0/0
     10.0.0.0/30 is subnetted, 4 subnets
C       10.0.2.0 is directly connected, FastEthernet0/0
O E2    10.0.3.0 [110/1] via 10.0.2.1, 00:22:16, FastEthernet0/0
O       10.0.2.4 [110/2] via 10.0.2.1, 00:29:13, FastEthernet0/0
O E2    10.0.3.4 [110/1] via 10.0.2.1, 00:22:16, FastEthernet0/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, Loopback0
O       192.168.1.2/32 [110/2] via 10.0.2.1, 00:29:25, FastEthernet0/0
O E2 192.168.2.0/24 [110/1] via 10.0.2.1, 00:22:28, FastEthernet0/0
```

```
CE2B#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     6.0.0.0/24 is subnetted, 1 subnets
O E2    6.6.6.0 [110/1] via 10.0.3.9, 00:25:17, FastEthernet0/0
     8.0.0.0/24 is subnetted, 1 subnets
C       8.8.8.0 is directly connected, Loopback0
     10.0.0.0/30 is subnetted, 4 subnets
O E2    10.0.2.8 [110/1] via 10.0.3.9, 00:25:17, FastEthernet0/0
C       10.0.3.8 is directly connected, FastEthernet0/0
O E2    10.0.2.12 [110/1] via 10.0.3.9, 00:25:17, FastEthernet0/0
O       10.0.3.12 [110/2] via 10.0.3.9, 00:25:17, FastEthernet0/0
     192.168.1.0/24 is variably subnetted, 3 subnets, 2 masks
O E2    192.168.1.1/32 [110/1] via 10.0.3.9, 00:25:29, FastEthernet0/0
O E2    192.168.1.0/24 [110/1] via 10.0.3.9, 00:25:29, FastEthernet0/0
O E2    192.168.1.2/32 [110/1] via 10.0.3.9, 00:25:29, FastEthernet0/0
O    192.168.2.0/24 [110/3] via 10.0.3.9, 00:25:35, FastEthernet0/0
```

6. Conclusiones

Este proyecto tiene por objetivo el estudio de las redes MPLS VPN. El análisis se ha estructurado en dos partes, una primera parte teórica, desarrollada en el capítulo ***2***, donde se han querido explicar brevemente las características y funcionalidades de estas redes, y una segunda parte, puntos ***3***, ***4*** y ***5***, que pretende ilustrar, de manera más práctica y mediante el desarrollo de dos topologías distintas, los conocimientos adquiridos previamente durante el estudio.

De igual manera, en este segundo tramo del trabajo, se expone la propuesta del enunciado de una práctica cuyas cuestiones están relacionadas con las dos topologías citadas anteriormente. Esta propuesta podrá, en un futuro, ser implementada como parte del plan de estudios de una asignatura universitaria de redes en cursos avanzados.

Este proyecto no tiene como finalidad dar a conocer en profundidad protocolos base como IP, OSPF o BGP, sino la de aportar un mayor conocimiento sobre los distintos métodos que ofrece MPLS junto a redes privadas VPN.

Se ha escogido la tecnología MPLS VPN como tema principal del ensayo debido a su gran popularidad entre las empresas tecnológicas, su creciente evolución dentro del sector y la cantidad de alternativas que ofrece -en estos años también se ha investigado acerca de, por ejemplo, redes IPv6 VPN sobre MPLS. Asimismo, durante el desarrollo de proyecto, se han podido observar otras ventajas de esta tecnología como su gran escalabilidad, flexibilidad, rendimiento, optimización del ancho de banda y facilidad en su configuración -el uso del protocolo BGP hace que tengas que configurar muy pocos elementos de la red para añadir una nueva sede.

La formación adquirida durante todos esos meses ha sido considerable. Tanto por lo que respecta a los conocimientos sobre este tipo de tecnologías, sus precedentes y su continua evolución, como a la enseñanza sobre las distintas aplicaciones software o emuladores de los que se puede hacer uso.

Por último, este trabajo ha alcanzado su objetivo principal basado en desarrollar una topología MPLS VPN que mejore y acompañe a la enseñanza de los alumnos a nivel práctico, dentro de los planes de estudios ahora existentes en la universidad.

Bibliografía

[1] “Understanding Layer 3 VPNs”
Juniper. https://www.juniper.net/documentation/en_US/junos/topics/concept/layer-3-vpn-overview.html (acceso: diciembre 2018)

[2] “Routing and Forwarding MPLS VPNs”
Power Game.
http://ww8.powergame.ml/?gkwrf=https%3A%2F%2Fwww.google.com%2F (acceso: enero 2019)

[3] “VPLS Overview”
Flylib.com. https://flylib.com/books/en/2.686.1/vpls_overview.html (acceso: enero 2019)

[4] “C7206VXR/400/GE CISCO 7206VXR with NPE-400 and GE+E I/O controller”
Econram Systems. https://www.econram.com/cisco-routers-c7206vxr-400-ge.html (acceso: febrero 2019)

[5] “Cisco 3660-MB-2FE 3600 Series Router Chassis with Power Supply”
Recycled Goods. https://www.recycledgoods.com/cisco-3660-mb-2fe-3600-series-router-chassis-with-power-supply/ (acceso: febrero 2019)

[6] E. Rosen, “Multiprotocol Label Switching Architecture”, Cisco Systems, Inc., RFC 3031, Enero 2001.

[7] E. Rosen, “BGP/MPLS IP Virtual Private Networks (VPNs)”, Cisco Systems, Inc., RFC 4364, Febrero 2006.

[8] E. Rosen, P. Psenak y P. Pillay-Esnault, “OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)”, Cisco Systems, Inc., RFC 4577, Junio 2006.

[9] M. Lasserre, Ed. Y V. Kompella, Ed., “Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling”, Alcatel-Lucent, RFC 4762, Enero 2007.

[10] K. Kompella, Ed. Y Y. Rekhter, Ed., “Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling”, Juniper Networks, RFC 4761, Enero 2007.

[11] Gavin Phillips. “The 5 major VPN protocols explained”

Make of Use. https://www.makeuseof.com/tag/major-vpn-protocols-explained/ (acceso: noviembre 2018)

[12] “MPLS VPN”
Cert. https://www.cert.uy/wps/wcm/connect/certuy/c3df385c-1582-4986-94b9-98c974496fbe/Presentaci%C3%B3n+02+-+MPLS-VPN.pdf?MOD=AJPERES (acceso: diciembre 2018)

[13] “Introduction to VPLS”
https://www.juniper.net/documentation/en_US/junos/topics/concept/vpn-vpls-introduction.html (acceso: enero 2019)

[14] “Acceso a las redes de comunicaciones electrónicas”
EUR-Lex. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM:l24108i (acceso: enero 2019)

[15] A. González Carrasco, “Integración y optimización de redes MPLS: Un caso práctico”, Tesis doctoral, Dpto. de Telecomunicaciones, Universidad Carlos III de Madrid, Madrid, España, 2011. [En línea]. Disponible en: https://e-archivo.uc3m.es/bitstream/handle/10016/20236/PFC_Alvaro_Gonzalez_Carrasco.pdf (acceso: marzo 2019)

[16] “MPLS: Layer 3 VPNs Configuration Guide”
Cisco. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_l3_vpns/configuration/xe-3s/mp-l3-vpns-xe-3s-book/mp-cfg-layer3-vpn.html (acceso: febrero 2019)

[17] L. Muñoz López y P. Antón Martínez, “Informe Anual del Sector TIC y de los Contenidos en España 2018”
Observatorio Nacional de las telecomunicaciones y de la SI.
https://www.ontsi.red.es/ontsi/sites/ontsi/files/InformeAnualSectorTICC2018.pdf (acceso: marzo 2019)

[18] “Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper”
Cisco VNI. https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html#_Toc532256808 (acceso: marzo 2019)

Anexo I: Configuración completa topología 1

P

```
interface Loopback0
 ip address 1.0.1.1 255.255.255.0
!
interface FastEthernet1/1
  ip address 10.0.0.5 255.255.255.252
  mpls ip
  no sh
!
interface FastEthernet1/0
  ip address 10.0.0.1 255.255.255.252
  mpls ip
  speed auto
  duplex auto
  no sh
!
interface FastEthernet0/0
  no ip address
  shutdown
  duplex full
!
router ospf 1
  router-id 1.0.1.1
  network 1.0.1.0 0.0.0.255 area 0
  network 10.0.0.0 0.0.0.3 area 0
  network 10.0.0.4 0.0.0.3 area 0
```

P1

```
interface Loopback0
  ip address 1.1.1.1 255.255.255.0
!
interface FastEthernet1/0
  ip address 10.0.0.1 255.255.255.252
  mpls ip
  speed auto
  duplex auto
!
interface FastEthernet0/0
  ip address 10.0.0.5 255.255.255.252
  mpls ip
!
router ospf 1
  router-id 1.1.1.1
  network 1.1.1.0 0.0.0.255 area 0
  network 10.0.0.0 0.0.0.3 area 0
  network 10.0.0.4 0.0.0.3 area 0
```

P2

```
interface Loopback0
  ip address 1.2.1.1 255.255.255.0
!
interface FastEthernet0/0
  ip address 10.0.0.6 255.255.255.252
  mpls ip
  speed auto
  duplex auto
!
interface FastEthernet1/0
  ip address 10.0.0.9 255.255.255.252
  mpls ip
!
router ospf 1
  router-id 1.2.1.1
  network 1.2.1.0 0.0.0.255 area 0
  network 10.0.0.4 0.0.0.3 area 0
  network 10.0.0.8 0.0.0.3 area 0
```

PE1

```
ip vrf userA
  rd 1:1
  route-target both 1:1

interface Loopback0
 ip address 2.2.2.2 255.255.255.0
```

PE2

```
ip vrf userA
       rd 1:1
       route-target both 1:1

interface Loopback0
 ip address 3.3.3.3 255.255.255.0
```

ip ospf network point-to-point ! interface FastEthernet0/0 ip address 10.0.0.2 255.255.255.252 duplex full mpls ip ! interface FastEthernet1/0 description connect to userA router ip vrf forwarding userA ip address 10.0.1.1 255.255.255.252 ip ospf 2 area 0 speed auto duplex auto ! router ospf 2 vrf userA router-id 10.0.1.1 net 10.0.1.0 0.0.0.3 area 0 capability vrf-lite redistribute bgp 1 subnets ! router ospf 1 router-id 2.2.2.2 network 2.2.2.0 0.0.0.255 area 0 network 10.0.0.0 0.0.0.3 area 0 ! router bgp 1 bgp log-neighbor-changes neighbor 3.3.3.3 remote-as 1 neighbor 3.3.3.3 update-source Loopback0 ! address-family vpnv4 neighbor 3.3.3.3 activate neighbor 3.3.3.3 send-community extended exit-address-family ! address-family ipv4 vrf userA redistribute ospf 2 exit-address-family !	ip ospf network point-to-point ! interface FastEthernet0/0 ip address 10.0.0.10 255.255.255.252 duplex full mpls ip ! interface FastEthernet1/0 description connect to userA router ip vrf forwarding userA ip address 10.0.2.1 255.255.255.252 ip ospf 2 area 0 speed auto duplex auto ! router ospf 2 vrf userA router-id 10.0.2.1 net 10.0.2.0 0.0.0.3 area 0 capability vrf-lite redistribute bgp 1 subnets ! router ospf 1 router-id 3.3.3.3 network 3.3.3.0 0.0.0.255 area 0 network 10.0.0.8 0.0.0.3 area 0 ! router bgp 1 bgp log-neighbor-changes neighbor 2.2.2.2 remote-as 1 neighbor 2.2.2.2 update-source Loopback0 ! address-family vpnv4 neighbor 2.2.2.2 activate neighbor 2.2.2.2 send-community extended exit-address-family ! address-family ipv4 vrf userA redistribute ospf 2 exit-address-family !
CE1	**CE2**
interface Loopback0 **ip address 5.5.5.5 255.255.255.0** **ip ospf network point-to-point** **ip ospf 1 area 0** **!** **interface FastEthernet0/0** **ip address 10.0.1.2 255.255.255.252** **ip ospf 1 area 0** **duplex auto** **speed auto** **!** **router ospf 1** **router-id 5.5.5.5** **log-adjacency-changes** **network 10.0.1.0 0.0.0.3 area 0**	interface Loopback0 ip address 6.6.6.6 255.255.255.0 ip ospf network point-to-point ip ospf 1 area 0 ! interface FastEthernet0/0 ip address 10.0.2.2 255.255.255.252 ip ospf 1 area 0 duplex auto speed auto ! router ospf 1 router-id 6.6.6.6 network 10.0.2.0 0.0.0.3 area 0 log-adjacency-changes

Tabla 7. Configuración completa topología 1

Anexo II: Presupuesto

En este punto, se exponen de manera detallada los costes estimados de la implementación del proyecto. Primeramente, se precisan los costes asociados a personal y posteriormente, los relacionados con el software y hardware utilizado. Finalmente, se concluirá con un coste estimado total.

- **PERSONAL:**

En este proyecto, se considerará como personal único el alumno. De este modo, se calcula su coste por hora para hallar el total. Como se muestra en el apartado *1.4*, los días totales invertidos son **163**, suponiendo una jornada parcial de cuatro horas diarias, incluyendo sábados y domingos, las horas totales invertidas son unas 652. Se asume, además, como salario de ingeniero junior, una media de 1350€ al mes.

Sueldo bruto mensual	1350€
Días trabajados al mes	24 días
Horas mensuales	96 h
Coste bruto/Hora trabajada	14€/h

Tabla 8. Sueldo del personal

Teniendo en cuenta la información anterior, el coste total de personal junior es:

Coste/Hora	Horas totales	Coste total
14€/h	652	9.128€

Tabla 9. Sueldo personal junior

Respecto al trabajo realizado por el tutor, suponiendo así el salario de ingeniero senior se obtiene:

Coste/Hora	Horas totales	Coste total
50€/h	20	1.000€

Tabla 10. Sueldo personal senior

- **SOFTWARE:**

Estos gastos están relacionados con las licencias necesarias usadas para el desarrollo completo del proyecto.

Software	Coste (€)
Windows 8	0
Microsoft Office 2010	0
NotePad	0
GNS3	0
Wireshark	0

Tabla 11. Coste de software

- **HARDWARE**

Como plataforma principal se sitúa un ordenador portátil HP con procesador Core i5, memoria RAM de 8GB y memoria en disco de 500GB.

Hardware	Coste (€)
Ordenador	520

Tabla 12. Coste de hardware

- **TOTAL:**

En este apartado, se indican los costes totales del proyecto incluyendo todos los anteriormente citados, un margen de riesgo (establecido al 10%) y el impuesto del Valor Añadido (IVA), hoy en día 21%.

		Coste (€)
Personal	*junior*	9.128€
	senior	1.000€
Software		0€
Hardware		520€
Riesgo (10%)		1.064,8€
IVA (21%)		2.236,08€
Total		**13.948,88€**

Tabla 13. Coste total

Anexo III: Resumen extendido en inglés

Motivation

Nowadays, MPLS VPN technology has become popular among ICT companies. This technology improves network's routers interconnectivity.

MPLS VPN platforms are used in many domains because of their high speed and low cost.

Thanks to MAN (*Metropolitan Area Network*) and WAN (*Wide Area Network*) networks, MPLS VPN networks ensure communication among different geographically isolated users. Customers seem to be members of the same LAN (*Local Area Network*).

Due to its efficient and secure transmissions, its applications reach from industrial networks to smartphones. They furthermore give the possibility of, for example, remote accesses or linking between different offices.

In an MPLS VPN topology, thanks to the set of different technologies and the corresponding control protocols, privacy in every user's network is achieved.

However, these new applications need additional requirements such as better security methods, scalability and reliability, ease of use and resource optimization.

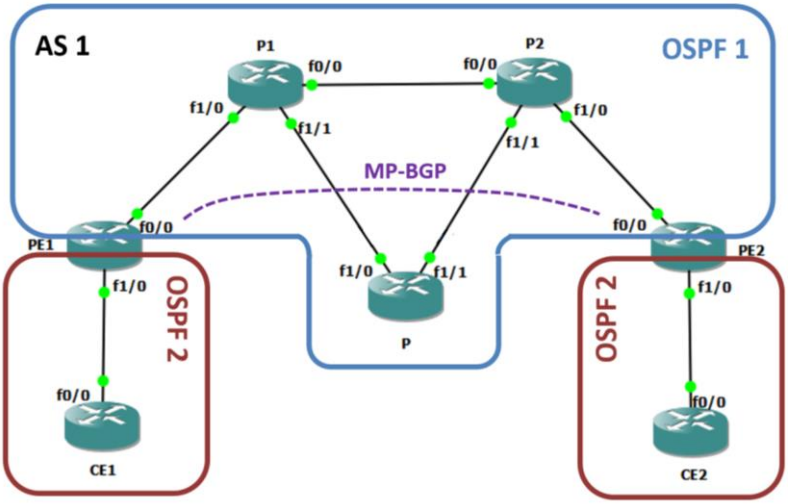
End user's needs make optimal and efficient the final design. Link and connectivity types are important elements of this analysis.

Objectives

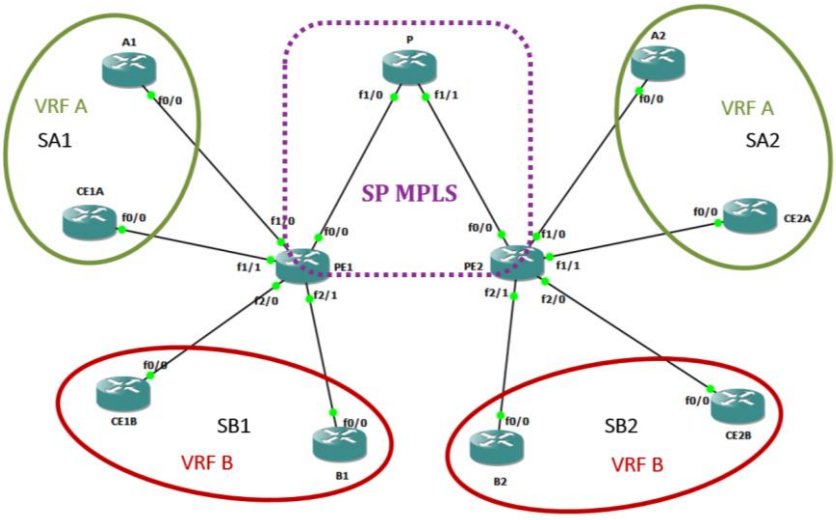
The main goal of this project aims at the analysis of the different level 3 private networks VPN within an MPLS architecture.

Firstly, the aim is to study all the features which describe an MPLS VPN network, both the 3 and the 2 level ones. This first part of the essay will begin by the MPLS protocol, which forms the backbone or service provider, and it will continue with the subsequent VPNs, which oversee the user's end-to-end communication.

Once all the necessary concepts have been studied, the research will focus on level 3 MPLS VPN topologies. First of all, we are going to observe the analysis and design of the network and secondly, the implementation of this prototype test, in an emulator. This topology model will offer a detailed practical knowledge about the defined above technologies.



To finish, a question wording model is defined as a future usable, practical tool in some Telematics Engineering subject´s curriculum. For this purpose, the first emulation is followed by several questions related to the implemented topology. Moreover, to add complexity to the practice, a second different topology will then be formulated. The student should complete its implementation.



The goal of this laboratory practice is to make the teaching of MPLS VPN technology more dynamic.

Social Environment

Telecommunications have experienced an upward trend in economic and social growth during recent years. Elements such as the number of companies committed to the sector, investment, active employment or business volume are in constant growth.

In 2017, the budget revenues of this sector were over 1.254.457 million € worldwide, 1,4% rather than year 2016.

However, in Spain, all these elements have suffered a further decline from past years. Within the ICT sector, telecommunication is the only area with a downward trend. Even so, the rapid increases since 2012 have placed it at the top-level of ICT areas: in 2017 there were 3.632 telecom companies which revenue exceeding the 27.904 million €.

Investment made by these companies in the market has experienced the most critical weakening, with a year-on-year decrease of 5,4%, to the end of 2017 the resulting loss of funding was about 265 million €. Finally, although the volume of business has also been reduced, it continues to be the area which generates most of the turnover in ICT market; retail services are the biggest contributors (78,6% of the total).

Thanks to the positive trend, which has been noted worldwide, there is no doubt about the constant evolution in every economic and social aspects of telecom industry. In fact, in the 2017-2022 period, it is estimated constant and persistent growth numbers for all the elements mentioned above. They expect to achieve a growth rate of 1,5% per year.

In the case of Spain, even with the low percentages collected in 2017, the most recent forecasts are altogether encouraging. A positive trend, even greater than the European one, is expected. While our country will be around the average global rate, Europe will be only in the 0,6%. This growth can be related to the progressive rise in public interest in foreign trades in ICT goods and services. Moreover, the investment from external companies is continually rising.

Traffic IP forecasts and trends

Once features, such as employment and turnover figures are known, we can start to evaluate the significant impact in other factors such as the IP network traffic.

The forecasts for 2022, according to the "*Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper*", are surprising. In the 2017-2022 period, the IP traffic growth will be higher than in the entire history of the Internet.

As can be seen from chart 1, IP traffic in 2022 would exceed more than three times that obtained in 2017; primarily result from wireless networks (71% of the total IP traffic in 2022).

In order to obtain a more in-depth analysis, IP traffic can be divided up in two big groups by the end user: **customers**, all the IP traffic generated by housing, universities…; and **business**, WAN IP traffic or the companies and government Internet. In 2022, the first group would constitute the 84% of the total while the second one would constitute the 16%. Internet traffic is the outstanding in both groups.

Conclusions

This research project aims to deepen the most important features of MPLS VPN networks known. The analysis has been segmented in two parts, an initial theoretical section in chapter ***2*** where the functionalities and characteristics of these networks are briefly explained, and a second section in chapters ***3***, ***4*** and ***5***, which has the purpose of illustrating, more practically, the knowledge acquired during the first part through the development of two different topology models. The question wording, based on these two topologies, is the most important part of this essay's second section. In the near future, this wording proposal may be implemented in advanced courses as part of a network's university subject's curriculum.

This project is not meant to provide detailed information on base protocols such as IP, OSPF or BGP, but rather has the mission of contributing with a better knowledge of MPLS technology and virtual private networks.

MPLS VPN technology has been chosen as the main topic of this essay because of its considerable popularity among ICT companies, its growing evolution within the area and the number of alternatives that offers -in these years, researches have been done on, for example, IPv6 VPN over MPLS networks. Moreover, during this project development, we have noticed some other advantages of this technology such as scalability, flexibility, high performance, bandwidth optimization and ease of configuration; using BGP protocol has reduced the number of configurations to make when adding a new site.

The training acquired during these months has been substantial. Both in regard to the knowledge about this type of technologies, its precedents and its continuous expansion, and the teaching on how to use different software apps or network support equipment.

To conclude, this essay has achieved its main goal of a topology MPLS VPN development which improves, on a practical level and along with the existing university curriculums, students' learning.